Vectorial types, non-determinism and probabilistic systems

Towards a computational quantum logic

Alejandro Díaz-Caro

Université Paris-Ouest Nanterre

INRIA Paris – Rocquencourt

Quantum Computing at Nancy

March 21, 2013

A proof-as-programs approach to quantum logic

Motivation

Curry-Howard correspondence

Intuitionistic logics $\Longleftrightarrow$ Typed λ-calculus

hypotheses	free variables
implication elimination (modus ponens)	application
implication introduction	abstraction

A proof is a program

(the formula it proves is a type for the program)

A proof-as-programs approach to quantum logic

Motivation

Curry-Howard correspondence

Intuitionistic logics $\Longleftrightarrow$ Typed λ-calculus

hypotheses	free variables
implication elimination (modus ponens)	application
implication introduction	abstraction

A proof is a program

(the formula it proves is a type for the program)

Goal: To find a *quantum* Curry-Howard correspondence

Between what?

- A *quantum* λ-calculus (quantum control/quantum data)
- Any logic, even if we need to define it!

A proof-as-programs approach to quantum logic

Motivation

Curry-Howard correspondence

Intuitionistic logics $\Longleftrightarrow$ Typed λ-calculus

hypotheses	free variables
implication elimination (modus ponens)	application
implication introduction	abstraction

A proof is a program

(the formula it proves is a type for the program)

Goal: To find a *quantum* Curry-Howard correspondence

Between what?

- A *quantum* λ-calculus (quantum control/quantum data)
- Any logic, even if we need to define it!

Computational quantum logic

We want a logic such that its proofs are quantum programs

Untyped algebraic extensions to λ-calculus

Two origins:

- *Alg* [Vaux'09] (from Linear Logic)
- *Lineal* [Arrighi,Dowek'08] (for Quantum computing)

Equivalent formalisms [Díaz-Caro,Perdrix,Tasson,Valiron'10]

Untyped algebraic extensions to λ-calculus

Two origins:

- *Alg* [Vaux'09] (from Linear Logic)
- *Lineal* [Arrighi,Dowek'08] (for Quantum computing)

Equivalent formalisms [Díaz-Caro,Perdrix,Tasson,Valiron'10]

$$\mathbf{t}, \mathbf{r} ::= \mathbf{v} \mid \mathbf{tr} \mid \mathbf{t} + \mathbf{r} \mid \alpha.\mathbf{t} \mid 0 \quad \alpha \in (\mathcal{S}, +, \times), \text{ a ring}$$
$$\mathbf{v} ::= x \mid \lambda x.\mathbf{t}$$

Untyped algebraic extensions to λ-calculus

Two origins:

- *Alg* [Vaux'09] (from Linear Logic)
- *Lineal* [Arrighi,Dowek'08] (for Quantum computing)

Equivalent formalisms [Díaz-Caro,Perdrix,Tasson,Valiron'10]

$$\mathbf{t}, \mathbf{r} ::= \mathbf{v} \mid \mathbf{tr} \mid \mathbf{t} + \mathbf{r} \mid \alpha.\mathbf{t} \mid 0 \quad \alpha \in (\mathcal{S}, +, \times), \text{ a ring}$$
$$\mathbf{v} ::= x \mid \lambda x.\mathbf{t}$$

$$\beta\text{-reduction: } (\lambda x.\mathbf{t})\mathbf{v} \to \mathbf{t}[x := \mathbf{v}]$$

"Algebraic" reductions:

$$\alpha.\mathbf{t} + \beta.\mathbf{t} \to (\alpha + \beta).\mathbf{t},$$
$$\alpha.\beta.\mathbf{t} \to (\alpha \times \beta).\mathbf{t},$$
$$\mathbf{t}(\mathbf{r}_1 + \mathbf{r}_2) \to \mathbf{tr}_1 + \mathbf{tr}_2,$$
$$(\mathbf{t}_1 + \mathbf{t}_2)\mathbf{r} \to \mathbf{t}_1\mathbf{r} + \mathbf{t}_2\mathbf{r},$$
$$\ldots$$

(oriented version of the axioms of vectorial spaces)

Untyped algebraic extensions to λ-calculus

Two origins:

- *Alg* [Vaux'09] (from Linear Logic)
- *Lineal* [Arrighi,Dowek'08] (for Quantum computing)

Equivalent formalisms [Díaz-Caro,Perdrix,Tasson,Valiron'10]

$$\mathbf{t}, \mathbf{r} ::= \mathbf{v} \mid \mathbf{tr} \mid \mathbf{t} + \mathbf{r} \mid \alpha.\mathbf{t} \mid 0 \quad \alpha \in (\mathcal{S}, +, \times), \text{ a ring}$$
$$\mathbf{v} ::= x \mid \lambda x.\mathbf{t}$$

$$\beta\text{-reduction: } (\lambda x.\mathbf{t})\mathbf{v} \to \mathbf{t}[x := \mathbf{v}]$$

"Algebraic" reductions:

$$\alpha.\mathbf{t} + \beta.\mathbf{t} \to (\alpha + \beta).\mathbf{t},$$
$$\alpha.\beta.\mathbf{t} \to (\alpha \times \beta).\mathbf{t},$$
$$\mathbf{t}(\mathbf{r}_1 + \mathbf{r}_2) \to \mathbf{tr}_1 + \mathbf{tr}_2,$$
$$(\mathbf{t}_1 + \mathbf{t}_2)\mathbf{r} \to \mathbf{t}_1\mathbf{r} + \mathbf{t}_2\mathbf{r},$$
$$\ldots$$

(oriented version of the axioms of vectorial spaces)

Vectorial space of values

$\mathcal{B} = \{ \text{ vars. and abs. } \}$

Space of values $::= \mathrm{Span}(\mathcal{B})$

Value == result of the computation, if it ends

Example: simple encoding of quantum computing

[Arrighi,Dowek'08]

Two base vectors: $|0\rangle = \lambda x.\lambda y.x$
$|1\rangle = \lambda x.\lambda y.y$

Example: simple encoding of quantum computing

[Arrighi,Dowek'08]

Two base vectors: $|0\rangle = \lambda x.\lambda y.x$, $|1\rangle = \lambda x.\lambda y.y$

We want a linear map H s.t.

$$H|0\rangle \to \overbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}^{|+\rangle}$$
$$H|1\rangle \to \underbrace{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)}_{|-\rangle}$$

Example: simple encoding of quantum computing

[Arrighi,Dowek'08]

Two base vectors: $|0\rangle = \lambda x.\lambda y.x$, $|1\rangle = \lambda x.\lambda y.y$

We want a linear map H s.t.

$$H|0\rangle \to \overbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}^{|+\rangle}$$
$$H|1\rangle \to \underbrace{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)}_{|-\rangle}$$

$$H := \lambda x.\{x\ [|+\rangle]\ [|-\rangle]\}$$

Example: simple encoding of quantum computing

[Arrighi,Dowek'08]

Two base vectors: $|0\rangle = \lambda x.\lambda y.x$, $|1\rangle = \lambda x.\lambda y.y$

We want a linear map H s.t.

$$H|0\rangle \to \overbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}^{|+\rangle}$$
$$H|1\rangle \to \underbrace{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)}_{|-\rangle}$$

$$\boxed{H \;:=\; \lambda x.\,\{x\;\;[|+\rangle]\;\;[|-\rangle]\}}$$

$$H|+\rangle = H(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \;\to\; \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) \;\to\; \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$$

$$= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \;\to\; \frac{1}{\sqrt{2}}(\sqrt{2}|0\rangle) \;\to\; |0\rangle$$

Typed *Lineal*: $\lambda^{\mathbf{vec}}$

[Arrighi,Díaz-Caro,Valiron'12]

$$
\begin{array}{rcl}
T, R & ::= & U \mid \mathbb{X} \mid \alpha.T \mid T + R \\
U & ::= & \mathsf{X} \mid U \to T \mid \forall \mathsf{X}.U \mid \forall \mathbb{X}.U
\end{array}
$$

$$
\begin{array}{rcl}
T + R & \equiv & R + T \\
T + (R + S) & \equiv & (T + R) + S \\
1.T & \equiv & T \\
\alpha.(\beta.T) & \equiv & (\alpha \times \beta).T \\
\alpha.T + \alpha.R & \equiv & \alpha.(T + R) \\
\alpha.T + \beta.T & \equiv & (\alpha + \beta).T
\end{array}
$$

Typed *Lineal*: λ^{vec}

[Arrighi,Díaz-Caro,Valiron'12]

$$\begin{array}{rcl} T, R & ::= & U \mid \mathbb{X} \mid \alpha.T \mid T + R \\ U & ::= & \mathsf{X} \mid U \to T \mid \forall \mathsf{X}.U \mid \forall \mathbb{X}.U \end{array}$$

$$\begin{array}{rcl} T + R & \equiv & R + T \\ T + (R + S) & \equiv & (T + R) + S \\ 1.T & \equiv & T \\ \alpha.(\beta.T) & \equiv & (\alpha \times \beta).T \\ \alpha.T + \alpha.R & \equiv & \alpha.(T + R) \\ \alpha.T + \beta.T & \equiv & (\alpha + \beta).T \end{array}$$

Most important property of λ^{vec}

$$\begin{array}{rcl} \Gamma \vdash \mathbf{t} : \sum_i \alpha_i.T_i & \Rightarrow & \mathbf{t} \to^* \sum_i \alpha_i.\mathbf{r}_i \\ \mathbf{t} \to^* \sum_i \alpha_i.\mathbf{r}_i & \Rightarrow & \Gamma \vdash \mathbf{t} : \sum_i \alpha_i.T_i + 0.R \end{array} \qquad \text{where } \Gamma \vdash \mathbf{r}_i : T_i$$

Typed *Lineal*: λ^{vec}

[Arrighi,Díaz-Caro,Valiron'12]

$$\begin{array}{rcl} T, R & ::= & U \mid \mathbb{X} \mid \alpha.T \mid T + R \\ U & ::= & \mathsf{X} \mid U \to T \mid \forall \mathsf{X}.U \mid \forall \mathbb{X}.U \end{array}$$

$$\begin{array}{rcl} T + R & \equiv & R + T \\ T + (R + S) & \equiv & (T + R) + S \\ 1.T & \equiv & T \\ \alpha.(\beta.T) & \equiv & (\alpha \times \beta).T \\ \alpha.T + \alpha.R & \equiv & \alpha.(T + R) \\ \alpha.T + \beta.T & \equiv & (\alpha + \beta).T \end{array}$$

Most important property of λ^{vec}

$$\begin{array}{rcl} \Gamma \vdash \mathbf{t} : \sum_i \alpha_i.T_i & \Rightarrow & \mathbf{t} \to^* \sum_i \alpha_i.\mathbf{r}_i \\ \mathbf{t} \to^* \sum_i \alpha_i.\mathbf{r}_i & \Rightarrow & \Gamma \vdash \mathbf{t} : \sum_i \alpha_i.T_i + 0.R \end{array} \qquad \text{where } \Gamma \vdash \mathbf{r}_i : T_i$$

A type system capturing the "vectorial" structure of terms

. . . to check for properties of probabilistic processes

. . . to check for properties of quantum processes

. . . or whatever application needing the structure of the vector

Typed *Lineal*: λ^{vec}

[Arrighi,Díaz-Caro,Valiron'12]

$$\begin{array}{rcl} T, R & ::= & U \mid \mathbb{X} \mid \alpha.T \mid T + R \\ U & ::= & \mathsf{X} \mid U \to T \mid \forall \mathsf{X}.U \mid \forall \mathbb{X}.U \end{array}$$

$$\begin{array}{rcl} T + R & \equiv & R + T \\ T + (R + S) & \equiv & (T + R) + S \\ 1.T & \equiv & T \\ \alpha.(\beta.T) & \equiv & (\alpha \times \beta).T \\ \alpha.T + \alpha.R & \equiv & \alpha.(T + R) \\ \alpha.T + \beta.T & \equiv & (\alpha + \beta).T \end{array}$$

Most important property of λ^{vec}

$$\begin{array}{rcl} \Gamma \vdash \mathbf{t} : \sum_i \alpha_i.T_i & \Rightarrow & \mathbf{t} \to^* \sum_i \alpha_i.\mathbf{r}_i \\ \mathbf{t} \to^* \sum_i \alpha_i.\mathbf{r}_i & \Rightarrow & \Gamma \vdash \mathbf{t} : \sum_i \alpha_i.T_i + 0.R \end{array} \qquad \text{where } \Gamma \vdash \mathbf{r}_i : T_i$$

A type system capturing the "vectorial" structure of terms

. . . to check for properties of probabilistic processes

. . . to check for properties of quantum processes

. . . or whatever application needing the structure of the vector

Still far from the main goal: (for a *quantum* Curry-Howard correspondence)

- $\lambda^{\mathrm{vec}} \longrightarrow$ "vectorial" programs (not only quantum)

Typed *Lineal*: λ^{vec}

[Arrighi,Díaz-Caro,Valiron'12]

$$\begin{array}{rcl} T, R & ::= & U \mid \mathbb{X} \mid \alpha.T \mid T + R \\ U & ::= & \mathsf{X} \mid U \to T \mid \forall \mathsf{X}.U \mid \forall \mathbb{X}.U \end{array}$$

$$\begin{array}{rcl} T + R & \equiv & R + T \\ T + (R + S) & \equiv & (T + R) + S \\ 1.T & \equiv & T \\ \alpha.(\beta.T) & \equiv & (\alpha \times \beta).T \\ \alpha.T + \alpha.R & \equiv & \alpha.(T + R) \\ \alpha.T + \beta.T & \equiv & (\alpha + \beta).T \end{array}$$

Most important property of λ^{vec}

$$\begin{array}{rcl} \Gamma \vdash \mathbf{t} : \sum_i \alpha_i.T_i & \Rightarrow & \mathbf{t} \to^* \sum_i \alpha_i.\mathbf{r}_i \\ \mathbf{t} \to^* \sum_i \alpha_i.\mathbf{r}_i & \Rightarrow & \Gamma \vdash \mathbf{t} : \sum_i \alpha_i.T_i + 0.R \end{array} \qquad \text{where } \Gamma \vdash \mathbf{r}_i : T_i$$

A type system capturing the "vectorial" structure of terms

. . . to check for properties of probabilistic processes

. . . to check for properties of quantum processes

. . . or whatever application needing the structure of the vector

Still far from the main goal: (for a *quantum* Curry-Howard correspondence)

- $\lambda^{\mathrm{vec}} \longrightarrow$ "vectorial" programs (not only quantum)
- The logic behind $\longrightarrow$ not easy to define

Non-determinism

Simplifying *Lineal*

$$\mathbf{t}, \mathbf{r} \ ::= \ x \mid \lambda x.\mathbf{t} \mid \mathbf{tr} \mid \mathbf{t} + \mathbf{r}$$

$$\mathbf{t} + \mathbf{r} \to \mathbf{t} \qquad\qquad \mathbf{t} + \mathbf{r} \to \mathbf{r}$$

Non-determinism

Simplifying *Lineal*

$$\mathbf{t}, \mathbf{r} \ ::= \ x \mid \lambda x.\mathbf{t} \mid \mathbf{tr} \mid \mathbf{t} + \mathbf{r}$$

$$\mathbf{t} + \mathbf{r} \to \mathbf{t} \qquad\qquad \mathbf{t} + \mathbf{r} \to \mathbf{r}$$

- Restricting to Linear Logic: Highly informative *quantitative* version of strong normalisation [Díaz-Caro,Manzonetto,Pagani'13]

Non-determinism

Simplifying *Lineal*

$$\mathbf{t}, \mathbf{r} \ ::= \ x \mid \lambda x.\mathbf{t} \mid \mathbf{tr} \mid \mathbf{t} + \mathbf{r}$$

$$\mathbf{t} + \mathbf{r} \to \mathbf{t} \qquad\qquad \mathbf{t} + \mathbf{r} \to \mathbf{r}$$

- Restricting to Linear Logic: Highly informative *quantitative* version of strong normalisation [Díaz-Caro,Manzonetto,Pagani'13]
  - However this is a restriction

Non-determinism

Simplifying *Lineal*

$$\mathbf{t}, \mathbf{r} \ ::= \ x \mid \lambda x.\mathbf{t} \mid \mathbf{tr} \mid \mathbf{t} + \mathbf{r}$$

$$\mathbf{t} + \mathbf{r} \to \mathbf{t} \qquad\qquad \mathbf{t} + \mathbf{r} \to \mathbf{r}$$

- Restricting to Linear Logic: Highly informative *quantitative* version of strong normalisation [Díaz-Caro,Manzonetto,Pagani'13]
  - However this is a restriction
- Full calculus: 2^{nd} order intuitionistic logic [Díaz-Caro,Petit'12]

Non-determinism

Simplifying *Lineal*

$$\mathbf{t}, \mathbf{r} \ ::= \ x \mid \lambda x.\mathbf{t} \mid \mathbf{tr} \mid \mathbf{t} + \mathbf{r}$$

$$\mathbf{t} + \mathbf{r} \to \mathbf{t} \qquad\qquad \mathbf{t} + \mathbf{r} \to \mathbf{r}$$

- Restricting to Linear Logic: Highly informative *quantitative* version of strong normalisation [Díaz-Caro,Manzonetto,Pagani'13]
  - However this is a restriction
- Full calculus: 2^{nd} order intuitionistic logic [Díaz-Caro,Petit'12]
  - 2^{nd} order intuitionistic logic $\leftrightarrow$ A non linear fragment of Linear Logic
  - First logic related to (a fragment of) *Lineal*

Non-determinism

[Díaz-Caro,Dowek'12-13]

$\mathbf{t} + \mathbf{r} \to \mathbf{t}$ and $\mathbf{t} + \mathbf{r} \to \mathbf{r}$ Uncontrolled non-determinism

Non-determinism

[Díaz-Caro,Dowek'12-13]

$\mathbf{t} + \mathbf{r} \to \mathbf{t}$ and $\mathbf{t} + \mathbf{r} \to \mathbf{r}$	Uncontrolled non-determinism
$\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{t}$ and $\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{r}$	A projector controlling it

Non-determinism

[Díaz-Caro,Dowek'12-13]

$\mathbf{t} + \mathbf{r} \to \mathbf{t}$ and $\mathbf{t} + \mathbf{r} \to \mathbf{r}$	Uncontrolled non-determinism
$\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{t}$ and $\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{r}$	A projector controlling it

Non-determinism naturally arise by considering some isomorphisms between propositions to be equivalences

Non-determinism

[Díaz-Caro,Dowek'12-13]

$\mathbf{t} + \mathbf{r} \to \mathbf{t}$ and $\mathbf{t} + \mathbf{r} \to \mathbf{r}$	Uncontrolled non-determinism
$\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{t}$ and $\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{r}$	A projector controlling it

Non-determinism naturally arise by considering some isomorphisms between propositions to be equivalences

$A \wedge B \equiv B \wedge A$ We want $\mathbf{t} + \mathbf{r} = \mathbf{r} + \mathbf{t}$

Non-determinism

[Díaz-Caro,Dowek'12-13]

$\mathbf{t} + \mathbf{r} \to \mathbf{t}$ and $\mathbf{t} + \mathbf{r} \to \mathbf{r}$ Uncontrolled non-determinism

$\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{t}$ and $\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{r}$ A projector controlling it

Non-determinism naturally arise by considering some isomorphisms between propositions to be equivalences

$A \wedge B \equiv B \wedge A$ We want $\mathbf{t} + \mathbf{r} = \mathbf{r} + \mathbf{t}$

$\pi_1(\mathbf{t} + \mathbf{r})$ does not make any sense in this setting

Non-determinism

[Díaz-Caro,Dowek'12-13]

$\mathbf{t} + \mathbf{r} \to \mathbf{t}$ and $\mathbf{t} + \mathbf{r} \to \mathbf{r}$ Uncontrolled non-determinism

$\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{t}$ and $\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{r}$ A projector controlling it

Non-determinism naturally arise by considering some isomorphisms between propositions to be equivalences

$A \wedge B \equiv B \wedge A$ We want $\mathbf{t} + \mathbf{r} = \mathbf{r} + \mathbf{t}$

$\pi_1(\mathbf{t} + \mathbf{r})$ does not make any sense in this setting

Instead: $\pi_A(\mathbf{t} + \mathbf{r})$ (when $\mathbf{t} : A$ or $\mathbf{r} : A$)

Non-determinism

[Díaz-Caro,Dowek'12-13]

$\mathbf{t} + \mathbf{r} \to \mathbf{t}$ and $\mathbf{t} + \mathbf{r} \to \mathbf{r}$ Uncontrolled non-determinism

$\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{t}$ and $\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{r}$ A projector controlling it

Non-determinism naturally arise by considering some isomorphisms between propositions to be equivalences

$A \wedge B \equiv B \wedge A$ We want $\mathbf{t} + \mathbf{r} = \mathbf{r} + \mathbf{t}$

$\pi_1(\mathbf{t} + \mathbf{r})$ does not make any sense in this setting

Instead: $\pi_A(\mathbf{t} + \mathbf{r})$ (when $\mathbf{t} : A$ or $\mathbf{r} : A$)

If both have type A, then this is a non-deterministic projector

Non-determinism

[Díaz-Caro,Dowek'12-13]

$\mathbf{t} + \mathbf{r} \to \mathbf{t}$ and $\mathbf{t} + \mathbf{r} \to \mathbf{r}$ Uncontrolled non-determinism

$\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{t}$ and $\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{r}$ A projector controlling it

Non-determinism naturally arise by considering some isomorphisms between propositions to be equivalences

$A \wedge B \equiv B \wedge A$ We want $\mathbf{t} + \mathbf{r} = \mathbf{r} + \mathbf{t}$

$\pi_1(\mathbf{t} + \mathbf{r})$ does not make any sense in this setting

Instead: $\pi_A(\mathbf{t} + \mathbf{r})$ (when $\mathbf{t} : A$ or $\mathbf{r} : A$)

If both have type A, then this is a non-deterministic projector

$\boxed{\lambda_+}$

- A proof system where equivalent propositions get the same proofs

$$A \wedge B \equiv B \wedge A \qquad A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$$
$$A \Rightarrow (B \wedge C) \equiv (A \Rightarrow B) \wedge (A \Rightarrow C)$$

Non-determinism

[Díaz-Caro,Dowek'12-13]

$\mathbf{t} + \mathbf{r} \to \mathbf{t}$ and $\mathbf{t} + \mathbf{r} \to \mathbf{r}$ Uncontrolled non-determinism

$\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{t}$ and $\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{r}$ A projector controlling it

Non-determinism naturally arise by considering some isomorphisms between propositions to be equivalences

$A \wedge B \equiv B \wedge A$ We want $\mathbf{t} + \mathbf{r} = \mathbf{r} + \mathbf{t}$

$\pi_1(\mathbf{t} + \mathbf{r})$ does not make any sense in this setting

Instead: $\pi_A(\mathbf{t} + \mathbf{r})$ (when $\mathbf{t} : A$ or $\mathbf{r} : A$)

If both have type A, then this is a non-deterministic projector

$\boxed{\lambda_+}$

- A proof system where equivalent propositions get the same proofs

$$A \wedge B \equiv B \wedge A \qquad A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$$
$$A \Rightarrow (B \wedge C) \equiv (A \Rightarrow B) \wedge (A \Rightarrow C)$$

- Curry-Howard correspondence with 2^{nd} order intuitionistic logic
- Non-deterministic projector

Non-determinism

[Díaz-Caro,Dowek'12-13]

$\mathbf{t} + \mathbf{r} \to \mathbf{t}$ and $\mathbf{t} + \mathbf{r} \to \mathbf{r}$ Uncontrolled non-determinism

$\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{t}$ and $\pi(\mathbf{t} + \mathbf{r}) \to \mathbf{r}$ A projector controlling it

Non-determinism naturally arise by considering some isomorphisms between propositions to be equivalences

$A \wedge B \equiv B \wedge A$ We want $\mathbf{t} + \mathbf{r} = \mathbf{r} + \mathbf{t}$

$\pi_1(\mathbf{t} + \mathbf{r})$ does not make any sense in this setting

Instead: $\pi_A(\mathbf{t} + \mathbf{r})$ (when $\mathbf{t} : A$ or $\mathbf{r} : A$)

If both have type A, then this is a non-deterministic projector

$\boxed{\lambda_+}$

- A proof system where equivalent propositions get the same proofs

$$A \wedge B \equiv B \wedge A \qquad A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$$
$$A \Rightarrow (B \wedge C) \equiv (A \Rightarrow B) \wedge (A \Rightarrow C)$$

- Curry-Howard correspondence with 2^{nd} order intuitionistic logic
- Non-deterministic projector

From non-determinism to probabilities?

From non-determinism to probabilities

Work-in-progress (in collaboration with G. Dowek)

Premise: The algebraic calculi are too complex

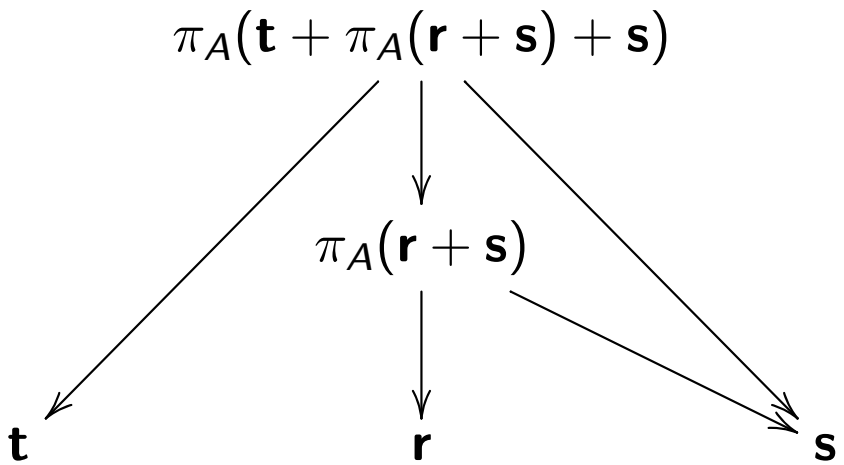
Do we really need them?

From non-determinism to probabilities

Work-in-progress (in collaboration with G. Dowek)

Premise: The algebraic calculi are too complex

Do we really need them?

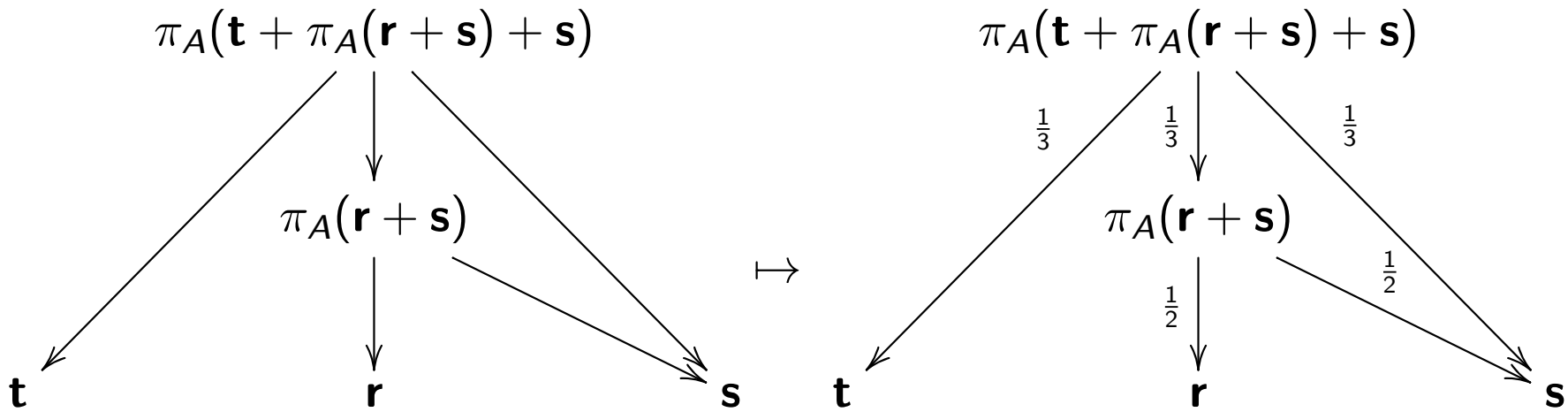


From non-determinism to probabilities

Work-in-progress (in collaboration with G. Dowek)

Premise: The algebraic calculi are too complex

Do we really need them?



$$\sim \quad \frac{1}{3}\mathbf{t} + \frac{1}{6}\mathbf{r} + \frac{1}{2}\mathbf{s}$$

From non-determinism to probabilities

Generalising for any non-deterministic abstract rewrite system

Definition (Oracle)

$f(\mathbf{a}) = \mathbf{b}$ if $\mathbf{a} \to \mathbf{b}$

$\Omega =$ set of all the oracles

$\left(\begin{array}{l} \text{if } \mathbf{a} \to \mathbf{b}_i \text{ with } i = 1, \ldots, n \\ \text{there are } n \text{ oracles} \end{array} \right)$

From non-determinism to probabilities

Generalising for any non-deterministic abstract rewrite system

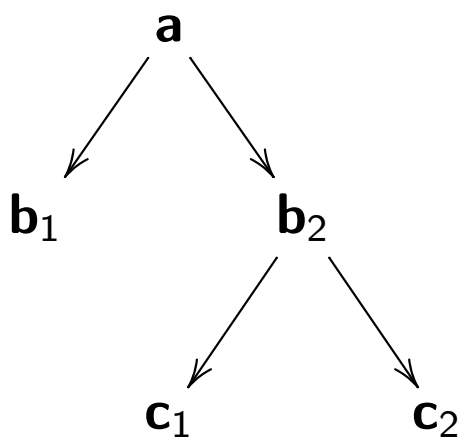
Definition (Oracle)

$f(\mathbf{a}) = \mathbf{b}$ if $\mathbf{a} \to \mathbf{b}$

Ω = set of all the oracles

$\left(\begin{array}{l} \text{if } \mathbf{a} \to \mathbf{b}_i \text{ with } i = 1, \ldots, n \\ \text{there are } n \text{ oracles} \end{array} \right)$

E.g. Rewrite system



$\Omega = \{f, g, h, i\}$, with

$$f(\mathbf{a}) = \mathbf{b}_1 \qquad g(\mathbf{a}) = \mathbf{b}_1$$
$$f(\mathbf{b}_2) = \mathbf{c}_1 \qquad g(\mathbf{b}_2) = \mathbf{c}_2$$

$$h(\mathbf{a}) = \mathbf{b}_2 \qquad i(\mathbf{a}) = \mathbf{b}_2$$
$$h(\mathbf{b}_2) = \mathbf{c}_1 \qquad i(\mathbf{b}_2) = \mathbf{c}_2$$

From non-determinism to probabilities

Theorem

$(\Omega, \mathcal{A}, P)$ *is a probability space*

- Ω is the set of all possible oracles
- $\mathcal{A}$ is the set of events (Lebesgue measurable subsets of Ω)
- P is the probability function (a Lebesgue measure over $\mathcal{A}$)

From non-determinism to probabilities

Theorem

$(\Omega, \mathcal{A}, P)$ *is a probability space*

- Ω is the set of all possible oracles
- $\mathcal{A}$ is the set of events (Lebesgue measurable subsets of Ω)
- P is the probability function (a Lebesgue measure over $\mathcal{A}$)

Work-in-progress:

Translation to/from $Lineal_{\mathbb{Q}}$ from/to λ_{+}^{p} [1]

[1] $Lineal_{\mathbb{Q}}$: *Lineal* in call-by-name, with scalars taken from $\mathbb{Q}^*$
λ_{+}^{p} : λ_{+} with probability rewriting

From non-determinism to probabilities

Theorem

$(\Omega, \mathcal{A}, P)$ *is a probability space*

- Ω is the set of all possible oracles
- $\mathcal{A}$ is the set of events (Lebesgue measurable subsets of Ω)
- P is the probability function (a Lebesgue measure over $\mathcal{A}$)

Work-in-progress:

Translation to/from $\mathit{Lineal}_{\mathbb{Q}}$ from/to λ_{+}^{p} [1]

Theorem (From $\mathit{Lineal}_{\mathbb{Q}}$ to λ_{+}^{p})

$$\boldsymbol{t} \to^{*} \sum_i p_i.\boldsymbol{r}_i \quad \Rightarrow \quad [\![\boldsymbol{t}]\!] \to^{*} [\![\boldsymbol{r}_i]\!] \text{ with probability } \frac{p_i}{p_1+\cdots+p_n}$$

Theorem (From λ_{+}^{p} to $\mathit{Lineal}_{\mathbb{Q}}$)

$$\boldsymbol{t} \to^{*} \boldsymbol{r}_i \text{ with probability } p_i, \text{ for } i = 1, \ldots, n \quad \Rightarrow \quad (\!|\boldsymbol{t}|\!) \to^{*} \sum_i p_i.(\!|\boldsymbol{r}_i|\!)$$

---

[1] $\mathit{Lineal}_{\mathbb{Q}}$: *Lineal* in call-by-name, with scalars taken from $\mathbb{Q}^{*}$
λ_{+}^{p} : λ_{+} with probability rewriting

Summarising

The long-term aim is to define a *computational* quantum logic

Summarising

The long-term aim is to define a *computational* quantum logic

We have

- A λ-calculus extension able to express quantum programs
- A complex type system characterising the structure of the vectors
- A linear non-deterministic model related to linear logic
- A Curry-Howard correspondence between λ_+ and 2^{nd} order intuitionistic logic
- An easy way to move from non-determinism to probabilities, without changing the model

Summarising

The long-term aim is to define a *computational* quantum logic

We have

- A λ-calculus extension able to express quantum programs
- A complex type system characterising the structure of the vectors
- A linear non-deterministic model related to linear logic
- A Curry-Howard correspondence between λ_+ and 2^{nd} order intuitionistic logic
- An easy way to move from non-determinism to probabilities, without changing the model

We need

- To move from probabilities to *quantum*, without loosing the connections to logic
  - No-cloning (Move back to call-by-value `[Arrighi,Dowek'08]`)
  - Measurement: we need to check for orthogonality
    $\alpha.M + \beta.N \to M$ with prob. $|\alpha|^2$, if $M \perp N$