Alejandro Díaz-Caro

Inria Nancy & Loria 🇫🇷
& Universidad Nacional de Quilmes 🇦🇷

The 31st International Conference on Types for Proofs and Programs (TYPES)
University of Strathclyde, Glasgow, Scotland • June 9–13, 2025

Motivation

Quantum proof language for some intuitionistic logic

Strategy

1. Modify a proof language to accommodate quantum programs
2. Modify a logic to accommodate quantum programs
3. Meet in the middle? Connect them somehow?

1.
Modify a proof language to accommodate quantum programs

Lambda-S: From quantum to logic

ADC, G. Dowek & J.P. Rinaldi. BioSystems (TPNC) 186:104012, 2019

Quantum computing: Unitary maps + measurement

Lambda-S: From quantum to logic

ADC, G. Dowek & J.P. Rinaldi. BioSystems (TPNC) 186:104012, 2019

Quantum computing: Unitary maps + measurement

Linearity by call-by-base strategy:

$$\underbrace{(\lambda x^A \,.\, t)}_{A\Rightarrow B}\ \underbrace{(\alpha \,.\, u + \beta \,.\, v)}_{S(A)} \longrightarrow \underbrace{\alpha \,.\, (\lambda x \,.\, t)\ u + \beta \,.\, (\lambda x \,.\, t)\ v}_{S(B)}$$

Lambda-S: From quantum to logic

ADC, G. Dowek & J.P. Rinaldi. BioSystems (TPNC) 186:104012, 2019

Quantum computing: Unitary maps + measurement

Linearity by call-by-base strategy:

$$\underbrace{(\lambda x^A\,.\,t)}_{A\Rightarrow B}\ \underbrace{(\alpha\,.\,u+\beta\,.\,v)}_{S(A)} \longrightarrow \underbrace{\alpha\,.\,(\lambda x\,.\,t)\ u+\beta\,.\,(\lambda x\,.\,t)\ v}_{S(B)}$$

Matrix $M := \begin{matrix} a & b \\ c & d \end{matrix}$ as a linear map:

$$M := \lambda x^{\texttt{bit}}\,.\,\texttt{if}\ x\ \texttt{then}\ (a\,.\,\texttt{true}+c\,.\,\texttt{false})\ \texttt{else}\ (b\,.\,\texttt{true}+d\,.\,\texttt{false})$$

$$M\ (\alpha\,.\,\texttt{true}+\beta\,.\,\texttt{false}) \longrightarrow \alpha\,.\,M\ \texttt{true}+\beta\,.\,M\ \texttt{false}$$

Lambda-S: From quantum to logic

ADC, G. Dowek & J.P. Rinaldi. BioSystems (TPNC) 186:104012, 2019

Quantum computing: Unitary maps + measurement

Linearity by call-by-base strategy:

$$\underbrace{(\lambda x^A . t)}_{A\Rightarrow B}\ \underbrace{(\alpha . u + \beta . v)}_{S(A)} \longrightarrow \underbrace{\alpha . (\lambda x . t)\ u + \beta . (\lambda x . t)\ v}_{S(B)}$$

Matrix $M := \begin{matrix} a & b \\ c & d \end{matrix}$ as a linear map:

$$M := \lambda x^{\texttt{bit}} . \texttt{if } x \texttt{ then } (a . \texttt{true} + c . \texttt{false}) \\ \texttt{else } (b . \texttt{true} + d . \texttt{false})$$

$$M\ (\alpha . \texttt{true} + \beta . \texttt{false}) \\ \longrightarrow \alpha . M\ \texttt{true} + \beta . M\ \texttt{false}$$

Non-linear maps, in Linear Logic style:

$$(\lambda x^{S(A)} . t)\ r \longrightarrow t[x := r]$$

where t uses x exactly once

Practical use:

measurement $\lambda x^{S(A)}$. meas x

Lambda-S: From quantum to logic

ADC, G. Dowek & J.P. Rinaldi. BioSystems (TPNC) 186:104012, 2019

Quantum computing: Unitary maps + measurement

Linearity by call-by-base strategy:

$$\underbrace{(\lambda x^A . t)}_{A\Rightarrow B}\ \underbrace{(\alpha . u + \beta . v)}_{S(A)} \longrightarrow \underbrace{\alpha . (\lambda x . t)\ u + \beta . (\lambda x . t)\ v}_{S(B)}$$

Matrix $M := \begin{matrix} a & b \\ c & d \end{matrix}$ as a linear map:

$$M := \lambda x^{\texttt{bit}} . \texttt{if}\ x\ \texttt{then}\ (a . \texttt{true} + c . \texttt{false})$$
$$\texttt{else}\ (b . \texttt{true} + d . \texttt{false})$$

$$M\ (\alpha . \texttt{true} + \beta . \texttt{false})$$
$$\longrightarrow \alpha . M\ \texttt{true} + \beta . M\ \texttt{false}$$

Non-linear maps, in Linear Logic style:

$$(\lambda x^{S(A)} . t)\ r \longrightarrow t[x := r]$$

where t uses x exactly once

Practical use:

measurement $\lambda x^{S(A)}$. meas x

Unitarity by a realisability model:

ADC, M. Guillermo, A. Miquel & B. Valiron. LICS 2019

Only norm-1 vectors valid in the model

Induces typing restrictions to ensure it

Lambda-S: From quantum to logic

ADC, G. Dowek & J.P. Rinaldi. BioSystems (TPNC) 186:104012, 2019

Quantum computing: Unitary maps + measurement

Linearity by call-by-base strategy:

$$\underbrace{(\lambda x^A . t)}_{A \Rightarrow B}\ \underbrace{(\alpha . u + \beta . v)}_{S(A)} \longrightarrow \underbrace{\alpha . (\lambda x . t)\ u + \beta . (\lambda x . t)\ v}_{S(B)}$$

Matrix $M := \begin{matrix} a & b \\ c & d \end{matrix}$ as a linear map:

$$M := \lambda x^{\mathtt{bit}} . \mathtt{if}\ x\ \mathtt{then}\ (a . \mathtt{true} + c . \mathtt{false})$$
$$\mathtt{else}\ (b . \mathtt{true} + d . \mathtt{false})$$

$$M\ (\alpha . \mathtt{true} + \beta . \mathtt{false})$$
$$\longrightarrow \alpha . M\ \mathtt{true} + \beta . M\ \mathtt{false}$$

Non-linear maps, in Linear Logic style:

$$(\lambda x^{S(A)} . t)\ r \longrightarrow t[x := r]$$

where t uses x exactly once

Practical use:
measurement $\lambda x^{S(A)}$. meas x

Unitarity by a realisability model:

ADC, M. Guillermo, A. Miquel & B. Valiron. LICS 2019

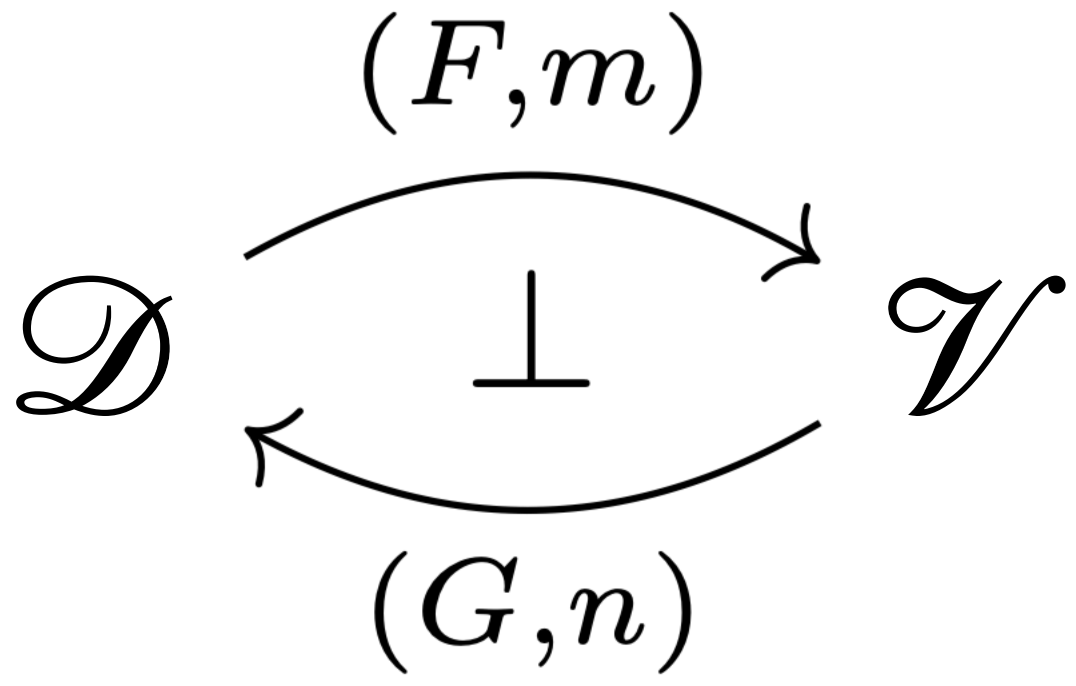
Only norm-1 vectors valid in the model
Induces typing restrictions to ensure it

Forced linearity for non-linear functions
Superpositions (non-duplicable terms) are treated linearly

Kind of oposite to Linear Logic

ADC, O. Malherbe. Applied Categorical Structures 28(5):807-844, 2020
ADC, O. Malherbe. Logical Methods in Computer Science 18(3:32), 2022
ADC, O. Malherbe. Mathematical Structures in Computer Science 34(1):1-44, 2023

Same adjunction as Linear Logic



- $\mathscr{D}$ cartesian closed category
- $\mathscr{V}$ additive symmetric monoidal closed category

Concrete example:

$\mathscr{D} = \mathbf{Set}$ $\quad F = \text{Span}$

$\mathscr{V} = \mathbf{Vec}$ $\quad G = \text{Forgetful functor}$

Lambda-S	**Linear Logic**
$[\![A]\!] \in \text{Obj}(\mathscr{D})$	$[\![A]\!] \in \text{Obj}(\mathscr{V})$
$[\![SA]\!] = GF[\![A]\!]$	$[\![\,!A]\!] = FG[\![A]\!]$

S marks non-duplicable data
$!$ marks duplicable data

2.
Modify a logic to accommodate quantum programs

Sup calculus: From logic to quantum

ADC, G. Dowek. Theoretical Computer Science 957:113840, 2023

Non-determinism in Logic

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\vdash C}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \odot B} \qquad \frac{\Gamma \vdash A \odot B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\vdash C}$$

Sup calculus: From logic to quantum

ADC, G. Dowek. Theoretical Computer Science 957:113840, 2023

Non-determinism in Logic

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\vdash C}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \odot B} \qquad \frac{\Gamma \vdash A \odot B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\vdash C}$$

Recovering determinism

$$\frac{\Gamma \vdash A \quad \Gamma \vdash A}{\Gamma \vdash A}$$

Sup calculus: From logic to quantum

ADC, G. Dowek. Theoretical Computer Science 957:113840, 2023

Non-determinism in Logic

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\vdash C}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \odot B} \qquad \frac{\Gamma \vdash A \odot B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\vdash C}$$

Recovering determinism

$$\frac{\Gamma \vdash A \quad \Gamma \vdash A}{\Gamma \vdash A}$$

Adding proof-terms

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash r : A}{\Gamma \vdash t + r : A}$$

Sup calculus: From logic to quantum

ADC, G. Dowek. Theoretical Computer Science 957:113840, 2023

Non-determinism in Logic

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\vdash C}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \odot B} \qquad \frac{\Gamma \vdash A \odot B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\vdash C}$$

Recovering determinism

$$\frac{\Gamma \vdash A \quad \Gamma \vdash A}{\Gamma \vdash A}$$

Adding proof-terms

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash r : A}{\Gamma \vdash t + r : A} \qquad \frac{\Gamma \vdash t : A}{\Gamma \vdash \alpha \cdot t : A} \qquad \frac{}{\Gamma \vdash \alpha . \star : \top}$$

Sup calculus: From logic to quantum

ADC, G. Dowek. Theoretical Computer Science 957:113840, 2023

Non-determinism in Logic

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\vdash C}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \odot B} \qquad \frac{\Gamma \vdash A \odot B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\vdash C}$$

Recovering determinism

$$\frac{\Gamma \vdash A \quad \Gamma \vdash A}{\Gamma \vdash A}$$

One-to-one correspondence:

$$\vdash v : \top \odot \top \odot \cdots \odot \top \Leftrightarrow \underline{v} \in \mathbb{C}^n$$

Adding proof-terms

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash r : A}{\Gamma \vdash t + r : A} \qquad \frac{\Gamma \vdash t : A}{\Gamma \vdash \alpha \cdot t : A} \qquad \frac{}{\Gamma \vdash \alpha . \star : \top}$$

Theorem: $\underline{v + w} = \underline{v} + \underline{w}$

$\underline{\alpha \cdot v} = \alpha \underline{v}$

Linear Sup Calculus

ADC, G. Dowek. Mathematical Structures in Computer Science, 34(10):1103-1137, 2024

$\odot$ as an additive connective

Connective	$\top$	$\bot$	$\Rightarrow$	$\wedge$	$\vee$	$\odot$
Additive	$\top$	0	$\Rightarrow$	$\&$	$\oplus$	$\odot$
Multiplicative	1	$\bot$	$\multimap$	$\otimes$	$\parr$	

Linear Sup Calculus

ADC, G. Dowek. Mathematical Structures in Computer Science, 34(10):1103-1137, 2024

$\odot$ as an additive connective

Connective	$\top$	$\bot$	$\Rightarrow$	$\wedge$	$\vee$	$\odot$
Additive	$\top$	0	$\Rightarrow$	$\&$	$\oplus$	$\odot$
Multiplicative	1	$\bot$	$\multimap$	$\otimes$	$⅋$	

Theorem:

$$f(\alpha \cdot t + \beta \cdot r) =_{obs} \alpha \cdot ft + \beta \cdot fr$$

Getting rid of $\odot$

ADC, G. Dowek. arXiv:502.19172, 2025

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \textsf{inl}\ t : A \oplus B} \qquad \frac{\Gamma \vdash r : B}{\Gamma \vdash \textsf{inr}\ r : A \oplus B}$$

$$\frac{\Gamma \vdash t : A \oplus B \quad \Delta, x : A \vdash s_1 : C \quad \Delta, y : B \vdash s_2 : C}{\Gamma, \Delta \vdash \textsf{match}\ t\ \textsf{in}\ \{x \mapsto s_1 \mid y \mapsto s_2\} : C}$$

Getting rid of ⊙

ADC, G. Dowek. arXiv:502.19172, 2025

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \mathsf{inl}\ t : A \oplus B} \qquad \frac{\Gamma \vdash r : B}{\Gamma \vdash \mathsf{inr}\ r : A \oplus B} \qquad \frac{\Gamma \vdash t : A \quad \Gamma \vdash r : B}{\Gamma \vdash \mathsf{inlr}(t, r) : A \oplus B}$$

$$\frac{\Gamma \vdash t : A \oplus B \quad \Delta, x : A \vdash s_1 : C \quad \Delta, y : B \vdash s_2 : C}{\Gamma, \Delta \vdash \mathsf{match}\ t\ \mathsf{in}\ \{x \mapsto s_1 \mid y \mapsto s_2\} : C}$$

Getting rid of $\odot$

ADC, G. Dowek. arXiv:502.19172, 2025

Same trick as before

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \mathsf{inl}\ t : A \oplus B} \qquad \frac{\Gamma \vdash r : B}{\Gamma \vdash \mathsf{inr}\ r : A \oplus B} \qquad \frac{\Gamma \vdash t : A \quad \Gamma \vdash r : B}{\Gamma \vdash \mathsf{inlr}(t, r) : A \oplus B} \qquad \frac{\Gamma \vdash t : A \quad \Gamma \vdash r : A}{\Gamma \vdash t + r : A}$$

$$\frac{\Gamma \vdash t : A \oplus B \quad \Delta, x : A \vdash s_1 : C \quad \Delta, y : B \vdash s_2 : C}{\Gamma, \Delta \vdash \mathsf{match}\ t\ \mathsf{in}\ \{x \mapsto s_1 \mid y \mapsto s_2\} : C} \qquad \frac{\Gamma \vdash \alpha \cdot t : A}{\Gamma \vdash t : A}$$

$$\frac{}{\Gamma \vdash \alpha . \star : 1}$$

Getting rid of $\odot$

ADC, G. Dowek. arXiv:502.19172, 2025

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \mathsf{inl}\ t : A \oplus B} \qquad \frac{\Gamma \vdash r : B}{\Gamma \vdash \mathsf{inr}\ r : A \oplus B} \qquad \frac{\Gamma \vdash t : A \quad \Gamma \vdash r : B}{\Gamma \vdash \mathsf{inlr}(t, r) : A \oplus B}$$

$$\frac{\Gamma \vdash t : A \oplus B \quad \Delta, x : A \vdash s_1 : C \quad \Delta, y : B \vdash s_2 : C}{\Gamma, \Delta \vdash \mathsf{match}\ t\ \mathsf{in}\ \{x \mapsto s_1 \mid y \mapsto s_2\} : C}$$

Same trick as before

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash r : A}{\Gamma \vdash t + r : A}$$

$$\frac{\Gamma \vdash \alpha \cdot t : A}{\Gamma \vdash t : A}$$

$$\frac{}{\Gamma \vdash \alpha . \star : 1}$$

In Linear Logic: Biproducts in an additive category do the trick

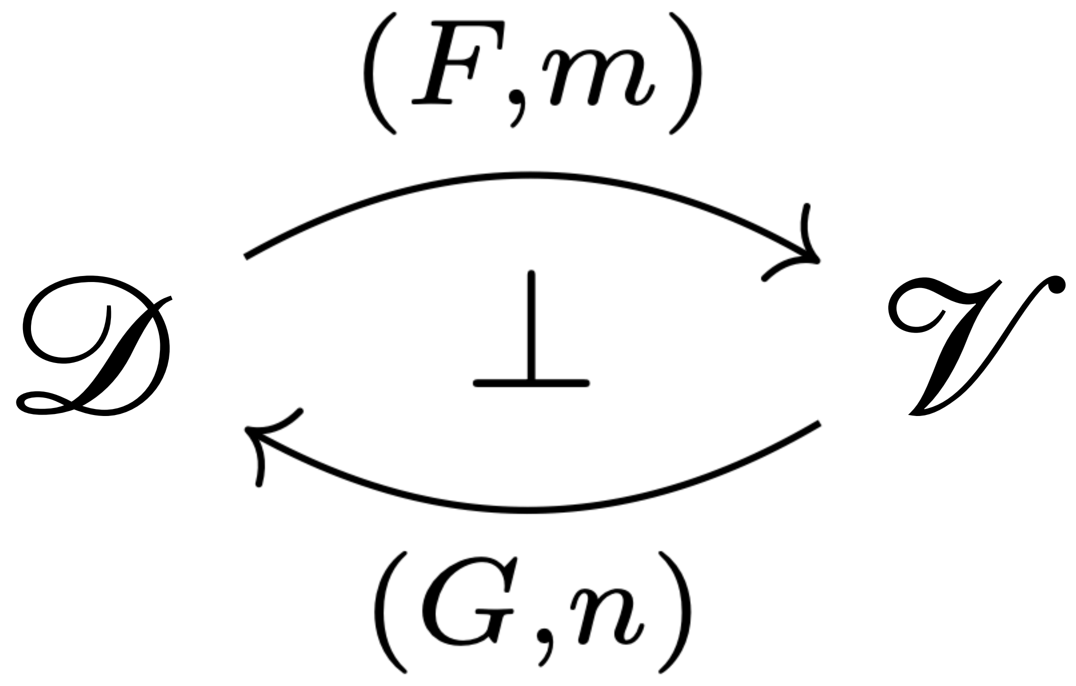
In Propositional Logic:

$$A \oplus B = (A \uplus B) \cup (A \times B)$$

ADC, O. Malherbe. arXiv:2408.16102, 2025

Summarising

Same adjunction as Linear Logic



- $\mathscr{D}$ cartesian closed category
- $\mathscr{V}$ additive symmetric monoidal closed category

Lambda-S

$[\![A]\!] \in \mathsf{Obj}(\mathscr{D})$

$[\![SA]\!] = GF[\![A]\!]$

Linear Sup$_!$ Calculus

ADC, G. Dowek, M. Ivnisky, O. Malherbe. WoLLIC 2024

$[\![A]\!] \in \mathsf{Obj}(\mathscr{V})$

$[\![\,!A]\!] = FG[\![A]\!]$

S marks non-duplicable data

$!$ marks duplicable data