A New Connective in Natural Deduction, and its Application to Quantum Computing

Alejandro Díaz-Caro and Gilles Dowek

- A new connective $\odot$ ("sup" for "superposition") in natural deduction
- A connective with *excessive* deduction rules
- The $\odot$-calculus: the proof-terms of propositional logic with $\odot$
- It contains the core of a quantum programming language

Harmony

Gentzen, inversion (Prawitz), harmony (Dummett)...

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-i}$$

$$\frac{\Gamma \vdash A \wedge B \quad \Gamma, A \vdash C}{\Gamma \vdash C} \wedge\text{-e1} \qquad \frac{\Gamma \vdash A \wedge B \quad \Gamma, B \vdash C}{\Gamma \vdash C} \wedge\text{-e2}$$

To prove $A \wedge B$, the introduction rule requires proofs of A and B

When we know $A \wedge B$, the elimination rules provides A and B as hypotheses

Same for the rules of disjunction, etc.

Proof reduction

Not specific to natural deduction: coherence for sequent calculus (Miller and Pimentel)

Disharmony I: insufficient deduction rules

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \textit{ tonk } B}\ \textit{tonk}\text{-i}$$

$$\frac{\Gamma \vdash A \textit{ tonk } B \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ \textit{tonk}\text{-e}$$

$2+2=4$, thus $2+2=4$ *tonk* $2+2=5$, thus $2+2=5$

No way to reduce the proof

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A}}{\Gamma \vdash A \textit{ tonk } B}\ \textit{tonk}\text{-i} \qquad \dfrac{\pi_2}{\Gamma, B \vdash C}}{\Gamma \vdash C}\ \textit{tonk}\text{-e}$$

Two good reasons to exclude *tonk*

Disharmony II: excessive deduction rules

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \odot B}\ \odot\text{-i}$$

$$\frac{\Gamma \vdash A \odot B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \odot\text{-e}$$

Many ways to reduce the proof

$$\frac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \odot B}\ \odot\text{-i} \quad \dfrac{\pi_3}{\Gamma, A \vdash C} \quad \dfrac{\pi_4}{\Gamma, B \vdash C}}{\Gamma \vdash C}\ \odot\text{-e}$$

- to $(\pi_1/A)\pi_3$
- to $(\pi_2/B)\pi_4$
- non deterministically either to $(\pi_1/A)\pi_3$ or to $(\pi_2/B)\pi_4$

Information loss

We must have π_1 and π_2 to build

$$\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \qquad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \odot B}\ \odot\text{-i}$$

Putting this proof in some context κ, we cannot get them both back

Excess of information required by introduction, not returned by elimination

Harmonious connectives: information preservation, reversibility, determinism
Excessive connectives: information loss, non reversibility, non determinism

Quantum measurement

We must have both $|\psi\rangle$ and $|\psi'\rangle$ to prepare the superposition

$$\frac{1}{\sqrt{2}}|\psi\rangle + \frac{1}{\sqrt{2}}|\psi'\rangle$$

With measurement, we cannot get both back

But only one (if performed in the basis $|\psi\rangle, |\psi'\rangle$)
in a non deterministic way
and the other is lost

Previous works

Superposition followed by measurement yields a reducible term $\pi(|\psi\rangle + |\psi'\rangle)$
Superposition is like introduction, measurement like elimination

But of which connective? ($\wedge$ or a close relative?)

Information loss: an excessive connective

Must have $|\psi\rangle$ and $|\psi'\rangle$ to build $|\psi\rangle + |\psi'\rangle$ (like $\wedge$)
But from $\pi(|\psi\rangle + |\psi'\rangle)$ only one back (like $\vee$)
Introduction rule of $\wedge$, elimination rule of $\vee$: $\odot$

A double face connective

$$\frac{\Gamma \vdash A \odot B \quad \Gamma, A \vdash C}{\Gamma \vdash C}\ \odot\text{-e1} \qquad \frac{\Gamma \vdash A \odot B \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \odot\text{-e2}$$

Three elimination rules

$\{\odot\text{-i}, \odot\text{-e}\}$ excessive rules

$\{\odot\text{-i}, \odot\text{-e1}, \odot\text{-e2}\}$ harmonious rules

Propositional logic with $\odot$

Proof terms

$$
\begin{aligned}
t = \ & x \mid \star \mid \delta_{\top}(t,u) \mid \delta_{\bot}(t) \mid \lambda x\ t \mid t\ u \\
& \mid \langle t,u\rangle \mid \delta^1_{\wedge}(t,x.u) \mid \delta^2_{\wedge}(t,x.u) \\
& \mid inl(t) \mid inr(t) \mid \delta_{\vee}(t,x.u,y.v) \\
& \mid [t,u] \mid \delta_{\odot}(t,x.u,y.v) \mid \delta^1_{\odot}(t,x.u) \mid \delta^2_{\odot}(t,x.u) \\
& \mid t \mathbin{\pmb{+}} u \mid \bullet t
\end{aligned}
$$

+ and •

Interstitial rules

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

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

Typing rules and reduction rules

For example

$$
\begin{aligned}
\delta_{\odot}([t,u], x.v, y.w) &\longrightarrow (t/x)v \\
\delta_{\odot}([t,u], x.v, y.w) &\longrightarrow (u/y)w \\
\delta^1_{\odot}([t,u], x.v) &\longrightarrow (t/x)v \\
\delta^2_{\odot}([t,u], x.v) &\longrightarrow (u/x)v \\
\\
\lambda x.t \boldsymbol{+} \lambda x.u &\longrightarrow \lambda x.(t \boldsymbol{+} u)
\end{aligned}
$$

Two theorems: Termination of proof reduction and Introduction property

Quantifying non-determinism

Computer scientists:

$$t \text{ reduces to } u_1 \text{ and to } u_2 \text{ in a non deterministic way}$$

The rest of the world:

$$t \text{ reduces to } u_1 \text{ with probability } \frac{1}{3} \text{ and to } u_2 \text{ with probability } \frac{2}{3}$$

A commutative field of scalars
Not one $\top$-i rule, but one for each scalar
Not one $\bullet$ rule, but one for each scalar

$$
\begin{array}{ll}
[\star, \star] & [1.\star, 2.\star] \\
\star \boldsymbol{+} \star \longrightarrow \star & 1.\star \boldsymbol{+} 2.\star \longrightarrow 3.\star \\
\bullet \star \longrightarrow \star & 2 \bullet 3.\star \longrightarrow 6.\star
\end{array}
$$

Application to ~~quantum~~ computing: Bits

$$\mathcal{B} = \top \vee \top$$

$$|0\rangle = inl(\star) \qquad |1\rangle = inr(\star)$$

Qubits

$$\mathcal{Q} = \top \odot \top$$

Qubit $a.|0\rangle + b.|1\rangle$ expressed as proof $[a.\star, b.\star]$

If $|\psi\rangle = [a.\star, b.\star]$, $|\psi'\rangle = [a'.\star, b'.\star]$
linear combination $c.|\psi\rangle + d.|\psi'\rangle$
But $c \bullet |\psi\rangle \boldsymbol{+} d \bullet |\psi'\rangle$ reduces to $[(ca + da').\star, (cb + db').\star]$

Measure

The information erasing, non reversible, and non deterministic proof constructor $\delta_\odot$

$$\pi'_1(t) = \delta_\odot(t, x.\mathbf{0}, y.\mathbf{1})$$

$\pi'_1([a.\star, b.\star])$ reduces to $\mathbf{0}$ with probability $\frac{|a|^2}{|a|^2+|b|^2}$, and $\mathbf{1}$ with probability $\frac{|b|^2}{|a|^2+|b|^2}$

Result of the measure
Others: state vector after the measure, partial measure on 2-qubits, etc.
A toolbox to build measurement operators

Matrices

Information preserving, reversible, and deterministic proof constructor $\delta^1_\odot$ and $\delta^2_\odot$

$$\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$$

expressed as

$$t = \lambda x.\delta^1_\odot(x, y.\delta_\top(y, [a.\star, b.\star])) \boldsymbol{+} \delta^2_\odot(x, z.\delta_\top(z, [c.\star, d.\star]))$$

$$\begin{aligned}
t\ [e.\star, f.\star] &\longrightarrow \delta^1_\odot([e.\star, f.\star], y.\delta_\top(y, [a.\star, b.\star])) \boldsymbol{+} \delta^2_\odot([e.\star, f.\star], z.\delta_\top(z, [c.\star, d.\star])) \\
&\longrightarrow^* \delta_\top(e.\star, [a.\star, b.\star]) \boldsymbol{+} \delta_\top(f.\star, [c.\star, d.\star]) \\
&\longrightarrow^* e \bullet [a.\star, b.\star] \boldsymbol{+} f \bullet [c.\star, d.\star] \\
&\longrightarrow^* [(a \times e).\star, (b \times e).\star] \boldsymbol{+} [(c \times f).\star, (d \times f).\star] \\
&\longrightarrow^* [(a \times e + c \times f).\star, ((b \times e + d \times f).\star]
\end{aligned}$$

Deutsch's algorithm

$$Deutsch = \lambda f.\pi_2'((H \otimes I)\ (U\ f\ \overline{|+-\rangle}))$$

On-going work

With the rules of natural deduction, matrices, but also non linear functions

A linear λ-calculus with $\odot$
The functions of $\mathcal{Q} \Rightarrow \mathcal{Q}$ (expressed without the $\delta_\odot$) are exactly the linear functions

Quantum computing is about information loss, not about information preservation