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
- An *excessive* connective
- The $\odot$-calculus: the proof-terms of propositional logic with $\odot$
- It contains the core of a quantum programming language
- But not a quantum logic: $\odot$ could be defined even if universe were not quantum

Harmony

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

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

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

When we know $A \wedge B$, the elimination rules gives us A and B

Same for disjunction

Gentzen, inversion (Prawitz), harmony (Dummett)...
Not specific to natural deduction: coherence for sequent calculus (Miller and Pimentel)

Harmony and cut elimination

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

reduces to $(\pi_1/A, \pi_2/B)\pi_3$

Disharmony I: insufficient connectives

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

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

$A =$ "$2 + 2 = 4$"
$B = C =$ "$2 + 2 = 5$"

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

No cut elimination for tonk

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A}}{\Gamma \vdash A \ \mathit{tonk}\ B}\ \mathit{tonk}\text{-i} \qquad \dfrac{\pi_3}{\Gamma, B \vdash C}}{\Gamma \vdash C}\ \mathit{tonk}\text{-e}$$

The information provided by the introduction rule is *insufficient* (B is expected and not provided by the introduction rule)

A good reason to exclude *tonk*

Disharmony II: excessive connectives

But also

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

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

The introduction rules require an excessive amount of information

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

can be reduced to $(\pi_1/A)\pi_3$

Another example

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

Many ways to reduce the cut

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

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

Why not keeping both proofs?

Add a structural rule

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

and reduce the cut to

$$\frac{\dfrac{(\pi_1/A)\pi_3}{\Gamma \vdash C} \qquad \dfrac{(\pi_2/B)\pi_4}{\Gamma \vdash C}}{\Gamma \vdash C}\ \text{parallel}$$

Information loss

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

Excess of information, required by introduction, not returned by elimination

The proof π_2 is present in the proof

$$\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \bullet B}\ \bullet\text{-i}$$

but it is not accessible: putting this proof in some context never yields a proof that reduces to π_2

Cut elimination erases it: after cut elimination, not even present

In the case of $\odot$

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

π_1 accessible, but only in a non deterministic way

In the case of $\odot$

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

reduces either

- non deterministically to π_1 or to $(\pi_2/B)\pi_3$
- or to

$$\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{(\pi_2/B)\pi_3}{\Gamma \vdash A}}{\Gamma \vdash A}\ \text{parallel}$$

still present, but still inaccessible

Quantum measure

$|\psi\rangle$ and $|\psi'\rangle$ two states

The superposition $|\psi\rangle + |\psi'\rangle$

Measurement of this superposition cannot yield both back

But only one (if performed in the basis $|\psi\rangle, |\psi'\rangle$)

In a non deterministic way

And the other is lost

(Some) quantum languages

Lineal (with Pablo): an untyped λ-calculus extended with linear combinations of terms

Lambda-$\mathcal{S}$ a typed version of a fragment of Lineal, with a measurement operator π
$\pi(t+u)$ reduces non deterministically to t or to u

System I: superposition $t+u$ the pair (t,u) (hence its type is a $\wedge$)
+ commutativity $(t,u)=(u,t)$ (type isomorphism)
A projection π_A: if $t:A$ and $u:B$, then $\pi_A(t+u)$ reduces to t and $\pi_B(t+u)$ to u
When $A=B$, proof-term $\pi_A(t+u)$ reduces, non deterministically, to t or to u

In the end of the day:
Superposition followed by measurement yields a reducible term $\pi(t+u)$
Superposition is like introduction, measurement like elimination

Connective?

Superposition is introduction, measurement is elimination
But of which connective?

$\wedge$?

$\pi(t + u)$ reduces non deterministically to t or to u erasing the other

An excessive connective

To build $t + u$, need both (like $\wedge$, hence our attempt)
But from $\pi(t + u)$ yields only one back (like $\vee$)
Introduction rule of $\wedge$, elimination rule of $\vee$: $\odot$

Propositional logic with $\odot$: proof terms

$$
\begin{aligned}
t = \;& x \mid * \mid \delta_{\bot}(t) \mid \lambda x\ t \mid t\ u \\
& \mid (t, u) \mid \delta_{\wedge}(t, [x, y]u) \\
& \mid \mathit{inl}(t) \mid \mathit{inr}(t) \mid \delta_{\vee}(t, [x]u, [y]v) \\
& \mid t + u \mid \delta_{\odot}(t, [x]u, [y]v) \mid \delta^{\parallel}_{\odot}(t, [x]u, [y]v) \\
& \mid t \parallel u
\end{aligned}
$$

Propositional logic with $\odot$: typing rules

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash u : B}{\Gamma \vdash t + u : A \odot B}\ \odot\text{-i}$$

$$\frac{\Gamma \vdash t : A \odot B \quad \Gamma, x : A \vdash u : C \quad \Gamma, y : B \vdash v : C}{\Gamma \vdash \delta_{\odot}(t, [x]u, [y]v) : C}\ \odot\text{-e}$$

$$\frac{\Gamma \vdash t : A \odot B \quad \Gamma, x : A \vdash u : C \quad \Gamma, y : B \vdash v : C}{\Gamma \vdash \delta_{\odot}^{\parallel}(t, [x]u, [y]v) : C}\ \odot\text{-e}$$

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash u : A}{\Gamma \vdash t \parallel u : A}\ \text{parallel}$$

Propositional logic with $\odot$: reduction rules 1

$$
\begin{aligned}
(\lambda x\ t)\ u &\longrightarrow (u/x)t \\
\delta_{\wedge}((t,u),[x,y]v) &\longrightarrow (t/x,u/y)v \\
\delta_{\vee}(\mathit{inl}(t),[x]v,[y]w) &\longrightarrow (t/x)v \\
\delta_{\vee}(\mathit{inr}(u),[x]v,[y]w) &\longrightarrow (u/y)w
\end{aligned}
$$

$$
\begin{aligned}
\delta_{\odot}(t+u,[x]v,[y]w) &\longrightarrow (t/x)v \\
\delta_{\odot}(t+u,[x]v,[y]w) &\longrightarrow (u/y)w
\end{aligned}
$$

$$
\delta^{\parallel}_{\odot}(t+u,[x]v,[y]w) \longrightarrow (t/x)v \parallel (u/y)w
$$

Commuting cuts

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,\wedge\text{-i} \quad \dfrac{\dfrac{\pi_3}{\Gamma \vdash A} \quad \dfrac{\pi_4}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,\wedge\text{-i}}{\Gamma \vdash A \wedge B} \text{ parallel} \quad \dfrac{\dfrac{\pi_5}{\Gamma, A, B \vdash C}}{\Gamma \vdash C}\,\wedge\text{-e}$$

Commuting cut: commute parallel, with elimination below or with introduction above

Often: with elimination (introduction is not possible for $\vee$)
Here: with introduction (except for the $\vee$), better introduction property, avoid duplicate `random`

Propositional logic with $\odot$: reduction rules 2

$$
\begin{aligned}
(\lambda x\ t) \parallel (\lambda x\ u) &\longrightarrow \lambda x\ (t \parallel u) \\
(t, u) \parallel (v, w)\rangle &\longrightarrow (t \parallel v, u \parallel w) \\
\delta_{\vee}(t \parallel u, [x]v, [y]w) &\longrightarrow \delta_{\vee}(t, [x]v, [y]w) \parallel \delta_{\vee}(u, [x]v, [y]w) \\
(t + u) \parallel (v + w) &\longrightarrow (t \parallel v) + (u \parallel w)
\end{aligned}
$$

Propositional logic with $\odot$: reduction rules 3

$$t \parallel t \longrightarrow t$$

The main theorem

Proof reduction terminates

Business as usual (an extension of Tait's proof, even common lemmas)

- $t \in [\![A \wedge B]\!]$ if t strongly terminates and whenever it reduces to a proof of the form (u, v), then $u \in [\![A]\!]$ and $v \in [\![B]\!]$
- $t \in [\![A \odot B]\!]$ if t strongly terminates and whenever it reduces to a proof of the form $u + v$, then $u \in [\![A]\!]$ and $v \in [\![B]\!]$

To handle commuting cuts: Girard's ultra-reduction ($t \parallel u \longrightarrow t$)
Used in the adequacy lemma for $\parallel$: if $t_1 \in [\![A]\!]$ and $t_2 \in [\![A]\!]$, then $t_1 \parallel t_2 \in [\![A]\!]$.

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:

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

Quantifying non-determinism

A set of scalars (propensities, rather than probabilities)

~~$t + u$~~ $a.t + b.u$
~~$t \parallel u$~~ $a.t \parallel b.u$

Invisible for typing

And almost invisible for reduction

$$\delta_{\odot}(a.t + b.u, [x]v, [y]w) \longrightarrow (t/x)v$$
$$\delta_{\odot}(a.t + b.u, [x]v, [y]w) \longrightarrow (u/y)w$$

$$\delta_{\odot}^{\parallel}(a.t + b.u, [x]v, [y]w) \longrightarrow a.(t/x)v \parallel b.(u/y)w$$

$$a.(c.t + d.u) \parallel b.(e.v + f.w) \longrightarrow 1.(ac.t \parallel be.v) + 1.(ad.u \parallel bf.w)$$
$$a.(b.t \parallel c.t) \longrightarrow (a(b + c)).t$$

So, termination extends trivially: color-blind glasses

Application to ~~quantum~~ computing: Bits

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

$$|0\rangle = \mathit{inl}(*) \qquad |1\rangle = \mathit{inr}(*)$$

closed irreducible proofs of $\mathcal{B}$
Not the only ones: $1.\mathit{inl}(*) \parallel 1.\mathit{inr}(*)$

$$\mathcal{B}^2 = \mathcal{B} \wedge \mathcal{B}$$

$$|00\rangle = (|0\rangle, |0\rangle) \qquad |01\rangle = (|0\rangle, |1\rangle)$$
$$|10\rangle = (|1\rangle, |0\rangle) \qquad |11\rangle = (|1\rangle, |1\rangle)$$

Can be generalized to n-tuples

Qubits

For quantum computing: more primitive constructions: linear combinations and non deterministic reduction: $\odot$

Qubit $a.|0\rangle + b.|1\rangle$ expressed as proof $a.|0\rangle + b.|1\rangle$ of $\mathcal{Q} = \mathcal{B} \odot \mathcal{B}$

If $|\psi\rangle = a.|0\rangle + b.|1\rangle$, $|\psi'\rangle = a'.|0\rangle + b'.|1\rangle$ proofs of $\mathcal{Q}$, linear combination $c.|\psi\rangle + d.|\psi'\rangle$ $(= (ca + da').|0\rangle + (cb + db').|1\rangle)$ cannot be $c.|\psi\rangle + d.|\psi'\rangle$ (proof of $\mathcal{Q} \odot \mathcal{Q}$ and not $\mathcal{Q}$)

But $c.|\psi\rangle \parallel d.|\psi'\rangle$ reduces to $(ca + da').|0\rangle + (cb + db').|1\rangle$

2-qubit $a.|00\rangle + b.|01\rangle + c.|10\rangle + d.|11\rangle$ expressed as proof $1.(a.|00\rangle + b.|01\rangle) + 1.(c.|10\rangle + d.|11\rangle)$ of $\mathcal{Q}^{\otimes 2} = (\mathcal{B}^2 \odot \mathcal{B}^2) \odot (\mathcal{B}^2 \odot \mathcal{B}^2)$

Probabilities

Strategy: $\delta_\odot(t, [x]u, [y]v)$ reduces only when t closed irreducible

$$\delta_\odot(a.|0\rangle + b.|1\rangle, [x]v, [y]w) \longrightarrow (|0\rangle/x)v$$

with probability $\frac{|a|^2}{|a|^2+|b|^2}$

$$\delta_\odot(a.|0\rangle + b.|1\rangle, [x]v, [y]w) \longrightarrow (|1\rangle/y)w$$

with probability $\frac{|b|^2}{|a|^2+|b|^2}$

Same for $1.(a.|00\rangle + b.|01\rangle) + 1.(c.|10\rangle + d.|11\rangle)$

Otherwise, any probability

Measure

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

$$\pi(t) = \delta_{\odot}(t, [x]|0\rangle, [y]|1\rangle)$$

$\pi(a.|0\rangle + b.|1\rangle)$ reduces to $|0\rangle$ and $|1\rangle$ with probabilities $\frac{|a|^2}{|a|^2+|b|^2}$ and $\frac{|b|^2}{|a|^2+|b|^2}$
Result of the measure

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

Matrices

Information preserving, reversible, and deterministic proof constructor $\delta^{\parallel}_{\odot}$

Proof of $\mathcal{B} \Rightarrow \mathcal{Q}$, function mapping base vectors to arbitrary vectors

$$M = \begin{pmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{pmatrix}$$

mapping $|0\rangle$ to $M_0 = m_{00}.|0\rangle + m_{10}.|1\rangle$ and $|1\rangle$ to $M_1 = m_{01}.|0\rangle + m_{11}.|1\rangle$

$$M = \lambda x \; If(x, M_0, M_1) = \lambda x \; \delta_{\vee}(x, [\_]M_1, [\_]M_2)$$

Application of a matrix to a vector

In Lineal, in $(\lambda x\ t)\ (a.|0\rangle + b.|1\rangle)$ $\lambda x\ t$ distributes over the linear combination $a.(\lambda x\ t)\ |0\rangle + b.(\lambda x\ t)\ |1\rangle$
as the terms $|0\rangle$ and $|1\rangle$ are base vectors, the β-redices can be reduced
Here, β-reduction not restricted
Application of a matrix to a vector

$$app = \lambda M \lambda t\ \delta^{\|}_{\odot}(t, [x]M\ x, [y]M\ y)$$

$$\begin{aligned} App\ M\ (a.|0\rangle + b.|1\rangle) &\longrightarrow a.(M\ |0\rangle)\ \|\ b.(M\ |1\rangle) \\ &\longrightarrow^{*} a.(m_{00}.|0\rangle + m_{10}.|1\rangle)\ \|\ b.(m_{01}.|0\rangle + m_{11}.|1\rangle) \\ &\longrightarrow 1.(m_{00}a.|0\rangle\ \|\ m_{01}b.|0\rangle) + 1.(m_{10}a.|1\rangle\ \|\ m_{11}b.|1\rangle) \\ &\longrightarrow^{*} (m_{00}a + m_{01}b).|0\rangle + (m_{10}a + m_{11}b).|1\rangle \end{aligned}$$

Generalizes to 2-qubits

Deutsch's algorithm

$$|+-\rangle = 1.(\frac{1}{2}.|00\rangle + \frac{-1}{2}.|01\rangle) + 1.(\frac{1}{2}.|10\rangle + \frac{-1}{2}.|11\rangle)$$

$$U = \lambda f\ \lambda x\ \delta_{\wedge}\Big(x, [y, z]If(y, If(z, M_0, M_1), If(z, M_2, M_3))\Big)$$

$$M_0 = Qubits\ (|0\rangle, \oplus\ |0\rangle\ (f\ |0\rangle))$$
$$M_1 = Qubits\ (|0\rangle, \oplus\ |0\rangle\ (f\ |1\rangle))$$
$$M_2 = Qubits\ (|1\rangle, \oplus\ |1\rangle\ (f\ |0\rangle))$$
$$M_3 = Qubits\ (|1\rangle, \oplus\ |1\rangle\ (f\ |1\rangle))$$

$H \otimes I$ matrix defined with $m_{00} = m_{20} = m_{11} = m_{31} = m_{02} = m_{13} = \frac{1}{\sqrt{2}}$, $m_{22} = m_{33} = -\frac{1}{\sqrt{2}}$, and all the others 0

$$Deutsch = \lambda f\ \pi_2(App_2\ (H \otimes I)\ (App_2\ (U\ f)\ |+-\rangle))$$

Proofs of propositional logic enough to define $\mathcal{B}$ and functions from $\mathcal{B}^n$ to $\mathcal{B}$

Adding $\odot$ introduces linear combination and measure as primitive constructions

Not a quantum programming language *per se* (for instance nothing prevents cloning) but all the ingredients needed to build a quantum language within a proof language

As linear combination and measurement is about information loss, not information preservation