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

Alejandro Díaz-Caro[1,2] and Gilles Dowek[3]

[1] DCyT, Universidad Nacional de Quilmes, Argentina
[2] ICC, CONICET–Universidad de Buenos Aires, Argentina
Email: adiazcaro@icc.fcen.uba.ar
[3] Inria, ENS Paris-Saclay, France
Email: gilles.dowek@ens-paris-saclay.fr

Abstract. We investigate an unsuspected connection between non harmonious logical connectives, such as Prior's *tonk*, and quantum computing. We defend that non harmonious connectives model the information erasure, the non-reversibility, and the non-determinism that occur, among other places, in quantum measurement. We introduce a propositional logic with a non harmonious connective *sup* and show that its proof language forms the core of a quantum programming language.

1 Introduction

We investigate an unsuspected connection between non harmonious logical connectives, such as Prior's *tonk*, and quantum computing. We defend that non harmonious connectives model the information erasure, the non-reversibility, and the non-determinism that occur, among other places, in quantum measurement.

More concretely, we introduce a propositional logic with a non harmonious connective $\odot$ (read: "sup", for "superposition") and show that its proof language forms the core of a quantum programming language.

1.1 Insufficient, harmonious, and excessive connectives

In natural deduction, to prove a proposition C, the elimination rule of a connective $\triangle$ requires a proof of $A \triangle B$ and a proof of C using, as extra hypotheses, exactly the premises needed to prove the proposition $A \triangle B$, with the introduction rules of the connective $\triangle$. This principle of inversion, or of harmony, has been introduced by Gentzen [10] and developed, among others, by Prawitz [16] and Dummett [8] in natural deduction, by Miller and Pimentel [12] in sequent calculus, and by Read [18–20] for the rules of equality.

For example, to prove the proposition $A \wedge B$, the introduction rule, in the usual additive style, of the conjunction requires proofs of A and B

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

Hence, to prove a proposition C, the generalized elimination rule of the conjunction [14,15,21] requires a proof of $A \wedge B$ and one of C, using, as extra hypotheses, the propositions A and B

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

Here we shall say that the extra hypotheses A and B are *provided* by the elimination rule. This principle of inversion can thus be formulated as the fact that the propositions required by the introduction rule are the same as those provided by the elimination rule.

It enables the definition of a proof reduction process where the proof

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

reduces to $(\pi_1/A, \pi_2/B)\pi_3$, that is the proof π_3 where the use of the axiom rule with the propositions A and B have been replaced with the proofs π_1 and π_2 respectively.

In the same way, to prove the proposition $A \vee B$, the introduction rules of the disjunction require a proof of A or a proof of B

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \ \vee\text{-i1} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \ \vee\text{-i2}$$

hence, to prove a proposition C, the elimination rule of the disjunction requires a proof of $A \vee B$ and two proofs of C, one using, as extra hypothesis, the proposition A and the other the proposition B

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

and a proof reduction process can be defined in a similar way.

The property that the elimination rule provides exactly the propositions required by the introduction rules can be split in two properties that it provides no more and no less (called "harmony" and "reversed harmony" in [11]).

We can also imagine connectives that do not verify this inversion principle, either because the elimination rule provides propositions not required by the introduction rule, or because the introduction rule requires propositions not provided by the elimination rule, or both. When the propositions provided by the elimination rule are not all required by the introduction rule, we call the connective *insufficient*. When the propositions provided by the elimination rule are required by the introduction rule, but some propositions required by the introduction rule are not provided by the elimination rule we call it *excessive*.

An example of an *insufficient* connective is Prior's *tonk* [17], with the introduction and elimination rules being

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

where the elimination rule requires a proof of A *tonk* B and a proof of C, using the extra hypothesis B, that is not required in the proof of A *tonk* B, with the introduction rule. For such connectives, the following proof cannot be reduced

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

An example of an *excessive* connective is the connective $\bullet$ that has the same introduction rule as conjunction

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

but whose elimination rule requires a proof of $A \bullet B$ and a proof of C, using the extra hypothesis A, but not B, although, both were required by the introduction rule

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

This connective could also be defined, using the more common elimination rules of conjunction, as having the introduction rule of the conjunction but only one among its two elimination rules.

For such connectives, a proof reduction process can be defined, as the proof

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

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

Another example is the connective $\odot$ that has the introduction rule of the conjunction and the elimination rule of the disjunction

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

In this case also, proof can be reduced. Moreover, several proof reduction processes can be defined, exploiting, in different ways, the excess of the connective. For example, the proof

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

can be reduced to $(\pi_1/A)\pi_3$, it can be reduced to $(\pi_2/B)\pi_4$, it also can be reduced, non deterministically, either to $(\pi_1/A)\pi_3$ or to $(\pi_2/B)\pi_4$. Finally, to keep both proofs, we can add a rule "parallel"

$$\dfrac{\Gamma \vdash A \quad \Gamma \vdash A}{\Gamma \vdash A}\ \text{par}$$

and reduce it to

$$\dfrac{\dfrac{(\pi_1/A)\pi_3}{\Gamma \vdash C} \quad \dfrac{(\pi_2/B)\pi_4}{\Gamma \vdash C}}{\Gamma \vdash C}\ \text{par}$$

A final example is the quantifier $\exists\!\!\forall$, that has the introduction rule of the universal quantifier and the elimination rule of the existential quantifier

$$\dfrac{\Gamma \vdash A}{\Gamma \vdash \exists\!\!\forall x\ A}\ \exists\!\!\forall\text{-i } x \text{ not free in } \Gamma \qquad \dfrac{\Gamma \vdash \exists\!\!\forall x\ A \quad \Gamma, A \vdash C}{\Gamma \vdash C}\ \exists\!\!\forall\text{-e } x \text{ not free in } \Gamma, C$$

The quantifier ∇ [13], defined in sequent calculus rather than natural deduction, may also be considered as an excessive quantifier, as it has the right rule of the universal quantifier and the left rule of the existential one. But it involves a clever management of variable scoping, that we do not address here.

1.2 Information loss

With harmonious connectives, when a proof is built with an introduction rule, the information contained in the proofs of the premises of this rule is preserved. For example, the information contained in the proof π_1 is *present* in the proof π

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

in the sense that π_1 is a subproof of π. But it is moreover accessible. We say that a subproof π' at position p in π is *accessible*, if there exists a context κ, such that for all proofs π'', putting the proof $\pi[\pi'']_p$ where π'' is grafted at position p in π, in the context κ yields a proof $\kappa[\pi[\pi'']_p]$ that reduces to π''. Indeed, putting the proof

$$\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\ \wedge\text{-i} \qquad \text{in the context} \qquad \dfrac{\dfrac{[\,]}{\Gamma \vdash A \wedge B} \quad \dfrac{}{\Gamma, A, B \vdash A}\ \text{ax}}{\Gamma \vdash A}\ \wedge\text{-e}$$

yields the proof

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

that reduces to π_1. And the same holds for the proof π_2.

The situation is different with an excessive connective: the excess of information, required by the introduction rule, and not returned by the elimination rule in the form of an extra hypothesis, in the required proof of C, is lost. For example, the information contained in the proof π_2 is present in the proof π

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

but it is inaccessible, as there is no context κ, such that, for all π_2, putting the proof

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

in the context κ yields a proof that reduces to π_2.

The information contained in the proofs π_1 and π_2 is present in the proof

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

but its accessibility depends on the way we decide to reduce the proof

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

If we reduce it systematically to $(\pi_1/A)\pi_3$, then the information contained in π_1 is accessible, but that contained in π_2 is not. If we reduce it systematically to $(\pi_2/B)\pi_4$, then the information contained in π_2 is accessible, but not that contained in π_1. If we reduce it not deterministically to $(\pi_1/A)\pi_3$ or to $(\pi_2/B)\pi_4$, then the information contained in both π_1 and π_2 is accessible but non deterministically. If we reduce it to

$$\dfrac{\dfrac{(\pi_1/A)\pi_3}{\Gamma \vdash C} \quad \dfrac{(\pi_2/B)\pi_4}{\Gamma \vdash C}}{\Gamma \vdash C}\ \text{par}$$

then the information contained in both π_1 and π_2 is inaccessible.

Indeed, the information contained in the proof π_1 is present in the proof

$$\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash A}}{\Gamma \vdash A}\ \text{par}$$

but it is inaccessible, as there is no context κ, such that, for all π_1, putting the proof

$$\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash A}}{\Gamma \vdash A}\ \text{par}$$

in the context κ yields a proof that reduces to π_1. The same holds for π_2.

Note that, when the proof

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

is reduced, non deterministically, to $(\pi_1/A)\pi_3$ or to $(\pi_1/A)\pi_3$, the information contained in π_1 or that contained in π_2 is erased. It is not even present in the reduct. When it is reduced to

$$\dfrac{\dfrac{(\pi_1/A)\pi_3}{\Gamma \vdash C} \quad \dfrac{(\pi_2/B)\pi_4}{\Gamma \vdash C}}{\Gamma \vdash C}\ \text{par}$$

then the information is inaccessible, but it remains present in the proof.

So, while harmonious connectives, that verify the inversion principle, model information preservation, reversibility, and determinism, these excessive connectives, that do not verify the inversion principle, model information erasure, non-reversibility, and non-determinism. Such information erasure, non-reversibility, and non-determinism, occur, for example, in quantum physics, where the measurement of the superposition of two states does not yield both states back.

The introduction rules alone do not define the meaning of such non harmonious connectives, and neither do the elimination rules alone. The discrepancy between the meaning conferred by the introduction rules and the elimination rules, and the information loss it implies, are part of the meaning of such connectives.

1.3 Quantum physics and quantum languages

Several programming languages have been proposed to express quantum algorithms, for example [1–3, 5, 9, 22, 23]. The design of such quantum programming languages raises two main questions. The first is to take into account the linearity of unitary operators and for instance avoid cloning, and the second is to express the information erasure, non-reversibility, and non-determinism of measurement and, more generally, to give a logical account to superposition. The $\odot$ connective gives a new solution to this second problem. Qubits can be seen as proofs of the proposition $\top \odot \top$, in contrast with bits which are proofs of $\top \vee \top$, and measurement can be easily expressed with the elimination rule of $\odot$.

In previous work, we have attempted to give a logical account to superposition. The calculus Lambda-$\mathcal{S}$ [9] contains a primitive constructor $+$ and a primitive measurement symbol π, together with a rule reducing $\pi(t+u)$ non deterministically to t or to u. The superposition $t+u$ can be considered as the pair (t,u). Hence, it should have the type $A \wedge A$. In other words, it is a proof-term of the proposition $A \wedge A$. In System I [4], various type-isomorphisms have been introduced, in particular the commutativity isomorphism $A \wedge B \equiv B \wedge A$, hence $t+u \equiv u+t$. In such a system, where $A \wedge B$ and $B \wedge A$ are identical, it is not possible to define the two elimination rules, as the two usual projections rules π_1 and π_2 of the λ-calculus. They were replaced with a single projection parametrized with a proposition A: π_A, such that if $t : A$ and $u : B$ then $\pi_A(t+u)$ reduces to t and $\pi_B(t+u)$ to u. When $A = B$, hence t and u both have type A, the proof-term $\pi_A(t+u)$ reduces, non deterministically, to t or to u. Thus, this modified elimination rule behaves like a measurement operator.

These works on Lambda-$\mathcal{S}$ and System I brought to light the fact that the pair superposition / measurement, in a quantum programming language, behaves like a pair introduction / elimination, for some connective, in a proof language, as the succession of a superposition and a measurement yields a term that can be reduced. In System I, this connective was assumed to be a commutative conjunction, with a modified elimination rule, leading to a non deterministic reduction.

But, as the measurement of the superposition of two states does not yield both states back, this connective should probably be excessive. Moreover, as, to prepare the superposition $a.|0\rangle + b.|1\rangle$, we need both $|0\rangle$ and $|1\rangle$ and the measurement, in the basis $|0\rangle, |1\rangle$, yields either $|0\rangle$ or $|1\rangle$, this connective should have the introduction rule of the conjunction, and the elimination rule of the disjunction. Hence, is should be the connective $\odot$.

In this paper, we present a propositional logic with the connective $\odot$, a language of proof-terms, the $\odot$-calculus (read: "the sup-calculus"), for this logic, and we prove a proof normalization theorem (Section 2).

We then extend this calculus, introducing scalars to quantify the propensity of a proof to reduce to another (Section 3) and show (Section 4) that its proof language forms the core of a quantum programming language.

2 Propositional logic with $\odot$

We consider a constructive propositional logic with the usual connectives $\top$, $\bot$, $\Rightarrow$, $\wedge$, and $\vee$, (as usual, negation can be defined with $\neg A = (A \Rightarrow \bot)$), and the extra connective $\odot$.

2.1 Definition

The syntax of this logic is

$$A = \top \mid \bot \mid A \Rightarrow A \mid A \wedge A \mid A \vee A \mid A \odot A$$

and its deduction rules are given Figure 1.

2.2 Proof normalization

Redexes in this logic are the usual redexes for the connectives $\Rightarrow$, $\wedge$, and $\vee$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\,\Rightarrow\text{-i} \quad \dfrac{\pi_2}{\Gamma \vdash A}}{\Gamma \vdash B}\,\Rightarrow\text{-e} \qquad \text{that reduces to} \qquad (\pi_2/A)\pi_1$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,\wedge\text{-i} \quad \dfrac{\pi_3}{\Gamma, A, B \vdash C}}{\Gamma \vdash C}\,\wedge\text{-e} \qquad \text{that reduces to} \qquad (\pi_1/A, \pi_2/B)\pi_3$$

$$\frac{A \in \Gamma}{\Gamma \vdash A}\ \text{ax} \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash A}{\Gamma \vdash A}\ \text{par} \qquad \frac{}{\Gamma \vdash \top}\ \top\text{-i} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash C}\ \bot\text{-e}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow\text{-i} \qquad \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \Rightarrow\text{-e}$$

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

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee\text{-i1} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee\text{-i2} \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee\text{-e}$$

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

Fig. 1: The deduction rules of propositional logic with $\odot$

$$\frac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A}}{\Gamma \vdash A \vee B}\ \vee\text{-i1} \quad \dfrac{\pi_2}{\Gamma, A \vdash C} \quad \dfrac{\pi_3}{\Gamma, B \vdash C}}{\Gamma \vdash C}\ \vee\text{-e} \qquad \text{that reduces to} \qquad (\pi_1/A)\pi_2$$

and

$$\frac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash B}}{\Gamma \vdash A \vee B}\ \vee\text{-i2} \quad \dfrac{\pi_2}{\Gamma, A \vdash C} \quad \dfrac{\pi_3}{\Gamma, B \vdash C}}{\Gamma \vdash C}\ \vee\text{-e} \qquad \text{that reduces to} \qquad (\pi_1/B)\pi_3$$

and the redex for the connective $\odot$

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

that reduces, in some cases, non deterministically, to $(\pi_1/A)\pi_3$ or to $(\pi_2/B)\pi_4$, erasing some information, and in others, preserving information, to

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

Adding rules, such as the parallel rule, permits to build proofs that cannot be reduced, because the introduction rule of some connectives and its elimination rule are separated by the parallel rule, for example

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

Reducing such a proof requires rules to commute the parallel rule, either with the elimination rule below or with the introduction rules above.

As the commutation with the introduction rules above is not always possible, for example in the proof

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A}}{\Gamma \vdash A \vee B}\ \vee\text{-i1} \quad \dfrac{\dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \vee B}\ \vee\text{-i2}}{\Gamma \vdash A \vee B}\ \text{par}$$

the commutation with the elimination rule below is often preferred. In this paper, we favor the commutation of the parallel rule with the introduction rules, rather than with the elimination rules, whenever it is possible, that is for all connectives except disjunction. For example the proof

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\ \wedge\text{-i} \quad \dfrac{\dfrac{\pi_3}{\Gamma \vdash A} \quad \dfrac{\pi_4}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\ \wedge\text{-i}}{\Gamma \vdash A \wedge B}\ \text{par}$$

reduces to

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_3}{\Gamma \vdash A}}{\Gamma \vdash A}\ \text{par} \quad \dfrac{\dfrac{\pi_2}{\Gamma \vdash B} \quad \dfrac{\pi_4}{\Gamma \vdash B}}{\Gamma \vdash B}\ \text{par}}{\Gamma \vdash A \wedge B}\ \wedge\text{-i}$$

Such a commutation yields a stronger introduction property for the considered connective (see Theorem 2.2 below).

2.3 Proof-terms

We introduce a term language, the $\odot$-calculus, for the proofs in this logic. Its syntax is

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

The variables x express the proofs built with the axiom rule, the terms $t \parallel u$ those built with the parallel rule, the term $*$ that built with the $\top$-i rule, the terms $\delta_\bot(t)$ those built with the $\bot$-e rule, the terms $\lambda x\ t$ those built with the $\Rightarrow$-i rule, the terms $t\ u$ those built with the $\Rightarrow$-e rule, the terms (t,u) those built with the $\wedge$-i rule, the terms $\delta_\wedge(t,[x,y]u)$ those built with the $\wedge$-e rule, the terms $\mathit{inl}(t)$ those built with the $\vee$-i1 rule, the terms $\mathit{inr}(t)$ those built with the $\vee$-i2 rule, the terms $\delta_\vee(t,[x]u,[y]v)$ those built with the $\vee$-e rule, the terms $t+u$ those

$$\frac{x : A \in \Gamma}{\Gamma \vdash x : A}\ \text{ax} \qquad \frac{\Gamma \vdash t : A \quad \Gamma \vdash u : A}{\Gamma \vdash t \parallel u : A}\ \text{par} \qquad \frac{}{\Gamma \vdash * : \top}\ \top\text{-i} \qquad \frac{\Gamma \vdash t : \bot}{\Gamma \vdash \delta_\bot(t) : C}\ \bot\text{-e}$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x\ t : A \Rightarrow B}\ \Rightarrow\text{-i} \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash u : A}{\Gamma \vdash t\ u : B}\ \Rightarrow\text{-e}$$

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

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \mathit{inl}(t) : A \vee B}\ \vee\text{-i1} \qquad \frac{\Gamma \vdash t : B}{\Gamma \vdash \mathit{inr}(t) : A \vee B}\ \vee\text{-i2}$$

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

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

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

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

Fig. 2: The typing rules of the $\odot$-calculus

built with the $\odot$-i rule, and the terms $\delta_\odot(t, [x]u, [y]v)$ and $\delta^{\parallel}_\odot(t, [x]u, [y]v)$ those built with the $\odot$-e rule.

The proofs of the form $*$, $\lambda x\ t$, (t, u), $\mathit{inl}(t)$, $\mathit{inr}(t)$, and $t + u$ are called *introductions*, and those of the form $\delta_\bot(t)$, $t\ u$, $\delta_\wedge(t, [x, y]u)$, $\delta_\vee(t, [x]u, [y]v)$, $\delta_\odot(t, [x]u, [y]v)$, or $\delta^{\parallel}_\odot(t, [x]u, [y]v)$ *eliminations*. Variables and terms of the form $t \parallel u$ are neither introductions nor eliminations.

The typing rules of the $\odot$-calculus are given in Figure 2 and its reduction rules Figure 3. The reduction relation is defined as usual as the smallest contextual relation that contains $\sigma l \longrightarrow \sigma r$, for all rules $l \longrightarrow r$ and substitutions σ.

The following two theorems are proved in the long version arXiv'ed at [7].

Theorem 2.1 (Termination). *If $\Gamma \vdash t : A$, then t strongly terminates.*

Theorem 2.2 (Introduction). *Let t be a closed irreducible proof of A.*

- *If A has the form $\top$, then t has the form $*$.*
- *The proposition A is not $\bot$.*
- *If A has the form $B \Rightarrow C$, then t has the form $\lambda x : B\ u$.*
- *If A has the form $B \wedge C$, then t has the form (u, v).*
- *If A has the form $B \vee C$, then t has the form $\mathit{inl}(u)$, $\mathit{inr}(u)$, or $u \parallel v$.*
- *If A has the form $B \odot C$, then t has the form $u + v$.*

3 Quantifying non-determinism

When we have a non deterministic reduction system, we often want to quantify the propensity of a proof to reduce to another. To do so, we enrich the term

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

Fig. 3: The reduction rules of the $\odot$-calculus

language with scalars, so that sums become linear combinations. Our set S of scalars can be any set, containing an element 1, and equipped with addition and multiplication. In practice, it is often the case that S is the field $\mathbb{R}$ or $\mathbb{C}$.

We define the $\odot^S$-calculus (read: "the sup-S-calculus"), by extending the grammar of proofs, adding a category for weighted proofs

$$\phi = a.t$$

where a is a scalar and modifying the category of proofs as follows

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

where the arguments of $\parallel$ and $+$ are weighted proofs.

Note that even in the case where there is a scalar 0, we need a proof t of A to build the weighted proof $0.t$.

The typing rules are those of Figure 2 with an extra rule for weighted proofs

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash a.t : A}$$

The reduction rules are those of Figure 3 enriched with the scalars. They are given Figure 4. All these rules reduce proofs, except the last one that reduces weighted proofs. Note that the proof $a.t \parallel b.t$ is irreducible: only the weighted proof $1.(a.t \parallel b.t)$ reduces to $(a+b).t$.

The termination proof of the $\odot$-calculus extends directly to the $\odot^S$-calculus: it suffices to define a translation $^\circ$ from the $\odot^S$-calculus to the $\odot$-calculus, erasing

$$
\begin{aligned}
(\lambda x\ t)\ u &\longrightarrow (u/x)t\\
\delta_\wedge((t,u),[x,y]v) &\longrightarrow (t/x,u/y)v\\
\delta_\vee(inl(t),[x]v,[y]w) &\longrightarrow (t/x)v\\
\delta_\vee(inr(u),[x]v,[y]w) &\longrightarrow (u/y)w\\
\delta_\odot(a.t+b.u,[x]v,[y]w) &\longrightarrow (t/x)v\\
\delta_\odot(a.t+b.u,[x]v,[y]w) &\longrightarrow (u/y)w\\
\delta^{\parallel}_\odot(a.t+b.u,[x]v,[y]w) &\longrightarrow a.(t/x)v \parallel b.(u/y)w\\
\\
a.(\lambda x\ t) \parallel b.(\lambda x\ u) &\longrightarrow \lambda x\ (a.t \parallel b.u)\\
a.(t,u) \parallel b.(v,w) &\longrightarrow (a.t \parallel b.v, a.u \parallel b.w)\\
\delta_\vee(a.t \parallel b.u,[x]v,[y]w) &\longrightarrow a.\delta_\vee(t,[x]v,[y]w) \parallel b.\delta_\vee(u,[x]v,[y]w)\\
a.(c.t+d.u) \parallel b.(e.v+f.w) &\longrightarrow 1.(ac.t \parallel be.v) + 1.(ad.u \parallel bf.w)\\
\\
a.(b.t \parallel c.t) &\longrightarrow (a(b+c)).t
\end{aligned}
$$

Fig. 4: The reduction rules of the $\odot^S$-calculus

the scalars, and check that if $t \longrightarrow u$ in the $\odot^S$-calculus, then $t^\circ \longrightarrow u^\circ$ in the $\odot$-calculus.

We can now associate a probability, depending on $a.t+b.u$, to the reductions

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

and 1 to the other reductions.

4 Application to quantum computing

We now show that the $\odot^{\mathbb{C}}$-calculus, with a reduction strategy allowing to reduce the proofs of the form $\delta_\odot(t,[x]u,[y]v)$ only when t is closed and irreducible, contains the core of a small quantum programming language. Requiring t to be closed and irreducible to reduce the proof $\delta_\odot(t,[x]u,[y]v)$ permits to assign probabilities to the reductions of this proof.

In the examples below, we focus on algorithms on one qubit and on two qubits. The generalization to algorithms on n qubits is straightforward. Note that the binary connective $\odot$ is always use with two identical propositions: $A \odot A$.

4.1 Bits

Definition 4.1 (Bit). *Let $\mathcal{B} = \top \vee \top$. The proofs $\mathbf{0} = inl(*)$ and $\mathbf{1} = inr(*)$ are closed irreducible proofs of $\mathcal{B}$.*

Remark 4.1. The proofs $inl(*)$ and $inr(*)$ are not the only closed irreducible proofs of $\mathcal{B}$, for example $1.inl(*) \parallel 1.inr(*)$ also is.

Definition 4.2 (Test). *We let $If(a,b,c) = \delta_\vee(a,[x]b,[y]c)$ where x and y are variables not occurring in b and c. We have $If(\mathbf{0},b,c) \longrightarrow b$ and $If(\mathbf{1},b,c) \longrightarrow c$.*

Boolean operators on $\mathcal{B}$ can be easily defined, for example, the exclusive or is the proof $\oplus = \lambda x \lambda y\ If(x, y, If(y, \mathbf{1}, \mathbf{0}))$ of $\mathcal{B} \Rightarrow \mathcal{B} \Rightarrow \mathcal{B}$.

Definition 4.3 (2-bit). *Let $\mathcal{B}^2 = \mathcal{B} \wedge \mathcal{B}$. The closed irreducible proofs of $\mathcal{B}^2$, $(\mathbf{0}, \mathbf{0})$, $(\mathbf{0}, \mathbf{1})$, $(\mathbf{1}, \mathbf{0})$, and $(\mathbf{1}, \mathbf{1})$ are written $\mathbf{00}$, $\mathbf{01}$, $\mathbf{10}$, and $\mathbf{11}$.*

4.2 Qubits

Definition 4.4 (Qubit). *Let $\mathcal{Q} = \top \odot \top$. A qubit $a.|0\rangle + b.|1\rangle$ is expressed as the proof $a.* + b.*$ of $\mathcal{Q}$.*

Remark 4.2. If the qubits $|\psi\rangle = a.|0\rangle + b.|1\rangle$ and $|\psi'\rangle = a'.|0\rangle + b'.|1\rangle$ are expressed as proofs of $\mathcal{Q}$, then the qubit $c.|\psi\rangle + d.|\psi'\rangle$, that is $(ca + da').|0\rangle + (cb + db').|1\rangle$, cannot be expressed, in the $\odot^{\mathbb{C}}$-calculus, with a linear combination of $|\psi\rangle$ and $|\psi'\rangle$, as the result would be a proof of $\mathcal{Q} \odot \mathcal{Q}$, and not of $\mathcal{Q}$. In contrast, the proof $c.|\psi\rangle \parallel d.|\psi'\rangle$ of $\mathcal{Q}$, reduces, in several steps, to $(ca+da').* + (cb+db').*$.

Definition 4.5 (2-qubit). *Let $\mathcal{Q}^{\otimes 2} = (\top \odot \top) \odot (\top \odot \top)$. A 2-qubit $a.|00\rangle + b.|01\rangle + c.|10\rangle + d.|11\rangle$ is expressed as the proof $1.(a. * + b.*) + 1.(c. * + d.*)$ of $\mathcal{Q}^{\otimes 2}$.*

4.3 Probabilities

If t is a closed irreducible proof of $\mathcal{Q}$ of the form $a. * + b.*$, where a and b are not both 0, then we assign the probability

$\frac{|a|^2}{|a|^2+|b|^2}$ to the reduction $\delta_\odot(a. * + b.*, [x]v, [y]w) \longrightarrow (*/x)v$

and $\frac{|b|^2}{|a|^2+|b|^2}$ to the reduction $\delta_\odot(a. * + b.*, [x]v, [y]w) \longrightarrow (*/y)w$.

If $a = b = 0$, we associate any probability, for example $\frac{1}{2}$, to both reductions.

If t is a closed irreducible proof of $\mathcal{Q}^{\otimes 2}$ of the form $1.(a.* + b.*) + 1.(c.* + d.*)$ where a, b, c, and d are not all 0, then we assign the probability

$\frac{|a|^2+|b|^2}{|a|^2+|b|^2+|c|^2+|d|^2}$ to the reduction

$$\delta_\odot(1.(a. * + b.*) + 1.(c. * + d.*), [x]v, [y]w) \longrightarrow ((a. * + b.*)/x)v$$

and $\frac{|c|^2+|d|^2}{|a|^2+|b|^2+|c|^2+|d|^2}$ to the reduction

$$\delta_\odot(1.(a. * + b.*) + 1.(c. * + d.*), [x]v, [y]w) \longrightarrow ((c. * + d.*)/y)w$$

If a, b, c, and d are all 0, we associate any probability to the reductions.

4.4 Measure

The information erasing, non reversible, and non deterministic proof constructor $\delta_\odot$ permits to define various measurement operators Figure 5.

If t is an irreducible proof of $\mathcal{Q}$ of the form $a. * + b.*$, where a and b are not both 0, then the proof $\pi(a.* + b.*)$ of the proposition $\mathcal{B}$ reduces, with probabilities

$$\begin{aligned}
\pi(t) &= \delta_{\odot}(t, [_]\mathbf{0}, [_]\mathbf{1}) \\
\pi'(t) &= \delta_{\odot}(t, [x]1.x + 0.*, [y]0.* + 1.y) \\
\pi''(t) &= \delta_{\odot}(t, [x](\mathbf{0}, 1.x + 0.*), [y](\mathbf{1}, 0.* + 1.y)) \\
\\
\pi_2(t) &= \delta_{\odot}(t, [_]\mathbf{0}, [_]\mathbf{1}) \\
\pi'_2(t) &= \delta_{\odot}(t, [x]1.x + 1.(0.* + 0.*), [y]1.(0.* + 0.*) + 1.y) \\
\pi''_2(t) &= \delta_{\odot}(t, [x](\mathbf{0}, 1.x + 1.(0.* + 0.*)), [y](\mathbf{1}, 1.(0.* + 0.*) + 1.y))
\end{aligned}$$

Fig. 5: Measurement operators

$\frac{|a|^2}{|a|^2+|b|^2}$ and $\frac{|b|^2}{|a|^2+|b|^2}$, to $\mathbf{0}$ and to $\mathbf{1}$. It is the result of the measure. The proof $\pi'(a.* + b.*)$ of the proposition $\mathcal{Q}$ reduces, with the same probabilities as above, to $1.* + 0.*$ and to $0.* + 1.*$. It is the state vector after the measure. The proof $\pi''(a.|0\rangle + b.\mathbf{1})$ of the proposition $\mathcal{B} \wedge \mathcal{Q}$ reduces, with the same probabilities as above, to $(\mathbf{0}, 1.* + 0.*)$ and to $(\mathbf{1}, 0.* + 1.*)$. It is the pair formed with the result of the measure and the state vector after the measure.

If t is an irreducible proof of $\mathcal{Q}^{\otimes 2}$ of the form $1.(a.* + b.*) + 1.(c.* + d.*)$ where a, b, c, and d are not all 0, then the proof $\pi_2(t)$ of the proposition $\mathcal{B}$ reduces, with probabilities $\frac{|a|^2+|b|^2}{|a|^2+|b|^2+|c|^2+|d|^2}$ and $\frac{|c|^2+|d|^2}{|a|^2+|b|^2+|c|^2+|d|^2}$, to $\mathbf{0}$ and to $\mathbf{1}$. It is the result of the partial measure of the first qubit. The proof $\pi'_2(t)$ of the proposition $\mathcal{Q}^{\otimes 2}$ reduces, with the same probabilities as above, to $1.(a.* + b.*) + 1.(0.* + 0.*)$ and $1.(0.* + 0.*) + 1.(c.* + d.*)$). It is the state vector after the partial measure of the first qubit. The proof $\pi''_2(t)$ of the proposition $\mathcal{B} \wedge \mathcal{Q}^{\otimes 2}$ reduces, with the same probabilities as above, to $(\mathbf{0}, 1.(a.* + b.*) + 1.(0.* + 0.*))$ and to $(\mathbf{1}, 1.(0.* + 0.*) + 1.(c.* + d.*)))$. It is the pair formed with the result of the measure and the state vector after the partial measure of the first qubit.

4.5 Matrices

The information erasing, non reversible, and non deterministic measurement operators are expressed with $\delta_{\odot}$. The information preserving, reversible, and deterministic unitary operators are expressed with $\delta^{\|}_{\odot}$.

Definition 4.6 (Matrix in $\mathcal{Q}$). *A matrix is a proof of $\mathcal{B} \Rightarrow \mathcal{Q}$, that is a function mapping bits to qubits. The matrix $M = \left(\begin{smallmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{smallmatrix}\right)$ mapping $\mathbf{0}$ to $M_0 = m_{00}.* + m_{10}.*$ and $\mathbf{1}$ to $M_1 = m_{01}.* + m_{11}.*$ is expressed as*

$$M = \lambda x\ \mathit{If}(x, M_0, M_1)$$

Note that $M\mathbf{0} \longrightarrow \mathit{If}(\mathbf{0}, M_0, M_1) \longrightarrow M_0$. Similarly, $M\mathbf{1} \longrightarrow^* M_1$.

In Lineal [2], a matrix $\lambda x\ t$, mapping canonical base vectors to arbitrary vectors, extends to an arbitrary vector $a.|0\rangle + b.|1\rangle$ as follows. When reducing the term $(\lambda x\ t)\ (a.|0\rangle + b.|1\rangle)$, the term $\lambda x\ t$ distributes over the linear combination $a.|0\rangle + b.|1\rangle$, yielding the term $a.(\lambda x\ t)\ |0\rangle + b.(\lambda x\ t)\ |1\rangle$ where, as the terms $|0\rangle$

and $|1\rangle$ are base vectors, the β-redexes $(\lambda x\ t)\ |0\rangle$ and $(\lambda x\ t)\ |1\rangle$ can be reduced. So the whole term reduces to $a.(|0\rangle/x)t + b.(|1\rangle/x)t$.

In the $\odot^{\mathbb{C}}$-calculus, β-reduction is not restricted to base vectors, but the application of a matrix to a vector can be defined.

Definition 4.7 (Application of a matrix to a vector in $\mathcal{Q}$). *We let*

$$App = \lambda M \lambda t\ \delta^{\parallel}_{\odot}(t, [x]M\ \mathbf{0}, [y]M\ \mathbf{1})$$

If $M : \mathcal{B} \Rightarrow \mathcal{Q}$, then the proof $App\ M\ (a.*+b.*)$ reduces to $a.(M\ \mathbf{0}) \parallel b.(M\ \mathbf{1})$. Therefore if M is the expression of the matrix $\left(\begin{smallmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{smallmatrix}\right)$, as in Definition 4.6, we have $App\ M\ (a.*+b.*) \longrightarrow^* (am_{00} + bm_{01}).*+(am_{10} + bm_{11}).*$.

Definition 4.8 (Matrix in $\mathcal{Q}^{\otimes 2}$). *A matrix is a proof of $\mathcal{B}^2 \Rightarrow \mathcal{Q}^{\otimes 2}$, that is a function mapping 2-bits to 2-qubits. The matrix $M = (m_{ij})_{ij}$ is expressed as*

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

where $M_i = 1.(m_{0i}.*+m_{1i}.*) + 1.(m_{2i}.*+m_{3i}.*)$ is the i-th column of M.

Note that $M\mathbf{00} \longrightarrow^* M_0$, $M\mathbf{01} \longrightarrow^* M_1$, $M\mathbf{10} \longrightarrow^* M_2$, and $M\mathbf{11} \longrightarrow^* M_3$.

Definition 4.9. *Taking $m_{ii} = 1$ and $m_{ij} = 0$ for $i \neq j$ yields the proof Qubits of $\mathcal{B}^2 \Rightarrow \mathcal{Q}^{\otimes 2}$ mapping each 2-bit to the corresponding 2-qubit. For example*

$$Qubits\ \mathbf{10} \rightarrow^* 1.(0.*+0.*) + 1.(1.*+0.*)$$

Definition 4.10 (Application of a matrix to a vector in $\mathcal{Q}^{\otimes 2}$). *We let*

$$App_2 = \lambda M \lambda t\ \delta^{\parallel}_{\odot}(t, [y]\delta^{\parallel}_{\odot}(y, [\_]M\ \mathbf{00}, [\_]M\ \mathbf{01}), [z]\delta^{\parallel}_{\odot}(z, [\_]M\ \mathbf{10}, [\_]M\ \mathbf{11}))$$

Hence, if $|\psi\rangle = 1.(a.*+b.*) + 1.(c.*+d.*)$ and $M : \mathcal{B}^2 \Rightarrow \mathcal{Q}^{\otimes 2}$, we have

$$\begin{aligned} &App_2\ M\ |\psi\rangle \\ &\longrightarrow^* 1.\big((am_{00} + bm_{01} + cm_{02} + dm_{03}).*+(am_{10} + bm_{11} + cm_{12} + dm_{13}).*\big) \\ &\quad + 1.\big((am_{20} + bm_{21} + cm_{22} + dm_{23}).*+(am_{30} + bm_{31} + cm_{32} + dm_{33}).*\big) \end{aligned}$$

4.6 An example: Deutsch's algorithm

Deutsch's algorithm allows to decide whether a 1-bit to 1-bit function f is constant or not, applying an oracle U_f, implementing f, only once. It is an algorithm operating on 2-qubits. It proceeds in four steps. (1) Prepare the initial state $|+-\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$. (2) Apply to it the unitary operator U_f, defined by $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$ for $x, y \in \{0, 1\}$, where $\oplus$ is the exclusive or. (3) Apply to it the unitary operator $H \otimes I = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{smallmatrix}\right)$. (4) Measure the first qubit. The output is $|0\rangle$, if f is constant and $|1\rangle$ if it is not.

In the $\odot^{\mathbb{C}}$-calculus, the initial state is $|+-\rangle = 1.(\frac{1}{2}.*+\frac{-1}{2}.*)+1.(\frac{1}{2}.*+\frac{-1}{2}).*$ the operator mapping f to U_f is expressed as in Definition 4.8

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

with $M_0 = \mathit{Qubits}\ (\mathbf{0}, \oplus\ \mathbf{0}\ (f\ \mathbf{0}))$ $M_2 = \mathit{Qubits}\ (\mathbf{1}, \oplus\ \mathbf{0}\ (f\ \mathbf{1}))$
$M_1 = \mathit{Qubits}\ (\mathbf{0}, \oplus\ \mathbf{1}\ (f\ \mathbf{0}))$ $M_3 = \mathit{Qubits}\ (\mathbf{1}, \oplus\ \mathbf{1}\ (f\ \mathbf{1}))$

where *Qubits* is defined in Definition 4.9 and the exclusive or $\oplus$ in Section 4.1. The operator $H \otimes I$ is expressed as in Definition 4.8 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 other m_{ij} are 0.

Finally, Deutsch's algorithm is the proof of $(\mathcal{B} \Rightarrow \mathcal{B}) \Rightarrow \mathcal{B}$

$$\mathit{Deutsch} = \lambda f\ \pi_2(\mathit{App}_2\ (H \otimes I)\ (\mathit{App}_2\ (U\ f)\ |+-\rangle))$$

Given a constant function proof of $\mathcal{B} \Rightarrow \mathcal{B}$, we have $\mathit{Deutsch}\ f \to^* \mathbf{0}$, while if f if not constant, $\mathit{Deutsch}\ f \to^* \mathbf{1}$.

5 Conclusion

We have defined the notions of insufficient and excessive connectives in natural deduction, extended propositional logic with an excessive connective $\odot$, and investigated the properties of the proof language of the obtained logic. We leave open the question of the interpretation of this logic in a model, besides the obvious Lindenbaum algebra.

These notions of insufficient and excessive connectives are not specific to natural deduction and similar notions could be defined, for instance, in sequent calculus. In sequent calculus however, harmony can be defined in a stronger sense, that includes, not only the possibility to normalize proofs, but also to reduce the use of the axiom rule on non atomic propositions to smaller ones [12]: an analog of the η-expansion, but generalized to arbitrary connectives.

The $\odot^{\mathbb{C}}$-calculus, the proof language of this logic, can express all quantum circuits. However, it is not restricted to only quantum algorithms, since the $\odot$ connective addresses the question of the the information erasure, non-reversibility, and non-determinism of measurement, but not that of linearity. We leave for future work the restriction of the calculus to linear operators, forbidding, for example, the non-linear term $\lambda x\ \delta^{\|}_{\odot}(x, [\_]\delta^{\|}_{\odot}(x, [\_]\mathbf{00}, [\_]\mathbf{01}), [\_]\delta^{\|}_{\odot}(x, [\_]\mathbf{10}, [\_]\mathbf{11}))$ that expresses a cloning machine.

It is also possible to restrict to the fragment of the language where proofs of $\mathcal{Q} \Rightarrow \mathcal{Q}$ have the form $\lambda x\ (\mathit{App}\ M\ x)$, for some proof M of $\mathcal{B} \Rightarrow \mathcal{Q}$. Then, we can also enforce unitarity, following the methods of [1, 5, 6].

Acknowledgements

The authors want to thank Jean-Baptiste Joinet, Dale Miller, and Alberto Naibo for useful discussions.

References

1. T; Altenkirch and J. Grattage. A functional quantum programming language. In *Proceedings of LICS 2005*, pages 249–258. IEEE, 2005.
2. P. Arrighi and G. Dowek. Lineal: A linear-algebraic lambda-calculus. *Logical Methods in Computer Science*, 13(1), 2017.
3. B. Coecke and A. Kissinger. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, 2017.
4. A. Díaz-Caro and G. Dowek. Proof normalisation in a logic identifying isomorphic propositions. In H. Geuvers, editor, *4th International Conference on Formal Structures for Computation and Deduction (FSCD 2019)*, volume 131 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 14:1–14:23. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2019.
5. A. Díaz-Caro, M. Guillermo, A. Miquel, and B. Valiron. Realizability in the unitary sphere. In *Proceedings of the 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2019)*, pages 1–13, 2019.
6. A. Díaz-Caro and O. Malherbe. Quantum control in the unitary sphere: Lambda-$\int_1$ and its categorical model. Draft at `arXiv:2012.05887`, 2020.
7. Alejandro Díaz-Caro and Gilles Dowek. A new connective in natural deduction, and its application to quantum computing. Draft at `arXiv:2012.08994`, 2020.
8. M. Dummett. *The Logical basis of metaphysics*. Duckworth, 1991.
9. A. Díaz-Caro, G. Dowek, and J.P. Rinaldi. Two linearities for quantum computing in the lambda calculus. *Biosystems*, 2019.
10. G. Gentzen. Untersuchungen über das logische Schliessen. In M. Szabo, editor, *The Collected Papers of Gerhard Gentzen*, pages 68–131. North-Holland, 1969.
11. Bruno Jacinto and Stephen Read. General-elimination stability. *Studia Logica*, 105:361–405, 2017.
12. D. Miller and E. Pimentel. A formal framework for specifying sequent calculus proof systems. *Theoretical Computer Science*, 474:98–116, 2013.
13. D. Miller and A. Tiu. A proof theory for generic judgments. *ACM Transactions on Computational Logic*, 6:749–783, 10 2005.
14. S. Negri and J. von Plato. *Structural Proof Theory*. Cambridge University Press, 2008.
15. M. Parigot. Free deduction: an analysis of computations in classical logic. In *Proceedings of Russian Conference on Logic Programming*, Lecture Notes in Computer Science, pages 361–380. Springer, 1991.
16. D. Prawitz. *Natural deduction. A proof-theoretical study*. Almqvist & Wiksell, 1965.
17. A.N. Prior. The runabout inference-ticket. *Analysis*, 21(2):38–39, 1960.
18. S. Read. Identity and harmony. *Analysis*, 64:113–119, 2004.
19. S. Read. General-elimination harmony and the meaning of the logical constants. *Journal of Philosophical Logic*, 39:557–576, 2010.
20. S. Read. Identity and harmony revisited. https://www.st-andrews.ac.uk/~slr/identity_revisited.pdf, 2014.
21. P. Schroeder-Heister. A natural extension of Natural deduction. *The Journal of Symbolic Logic*, 49(4):1284–1300, 1984.
22. P. Selinger and B. Valiron. A lambda calculus for quantum computation with classical control. *Mathematical Structures in Computer Science*, 16(3):527–552, 2006.
23. M. Zorzi. On quantum lambda calculi: a foundational perspective. *Mathematical Structures in Computer Science*, 26(7):1107–1195, 2016.