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

Alejandro Díaz-Caro, Gilles Dowek

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

Alejandro Díaz-Caro[a,b], Gilles Dowek[c,d]

[a]*Departamento de Ciencia y Tecnología, Universidad Nacional de Quilmes, Argentina*
[b]*Instituto de Ciencias de la Computación, CONICET–Universidad de Buenos Aires, Argentina*
[c]*Inria, France*
[d]*École Normale Supérieure Paris-Saclay, France*

Abstract

We investigate an unsuspected connection between logical connectives with non-harmonious deduction rules, such as Prior's *tonk*, and quantum computing. We argue these 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 logical connective *sup* that has non-harmonious deduction rules and also with two interstitial rules, and show that the proof language of this logic forms the core of a quantum programming language.

Keywords: Proof-reduction, Lambda calculus, Type theory, Quantum computing
2020 MSC: 03F05, 68N18, 03B38, 03B70, 81P68

1. Introduction

We investigate an unsuspected connection between logical connectives with non-harmonious deduction rules, such as Prior's *tonk*, and quantum computing. We argue these 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 logical connective $\odot$ (read: "sup", for "superposition") that has non-harmonious deduction rules and also with two interstitial rules and show that the proof language of this logic forms the core of a quantum programming language.

1.1. Logical connectives with insufficient, harmonious, and excessive deduction rules

In natural deduction, to prove a proposition C, the elimination rules of a connective $\triangle$ require 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 [8] and developed, among others, by Prawitz [17] and Dummett [6] for natural deduction, by Miller and Pimentel [13] for sequent calculus, and by Read [19, 20, 21] for the rules of equality.

For example, to prove the proposition $A \wedge B$, the introduction rule of the conjunction

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

requires proofs of A and of B and, to prove a proposition C, the generalized elimination rules of the conjunction [22, 16, 15]

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

require a proof of $A \wedge B$ and one of C, using, as extra hypothesis, the proposition A for the first and B for the second.

We say that the extra hypotheses A and B are *provided* by the elimination rules, as they appear in the left-hand side of the premise. In the same way, we say that the propositions A and B are *required* by the introduction rules, as they appear in the right-hand side of the premises.

This principle of inversion can thus be formulated as the fact that the propositions required by the introduction rules are the same as those provided by the elimination rules. It enables the definition of a reduction process, where the proof

$$\frac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B} \; \wedge\text{-i} \quad \dfrac{\pi_3}{\Gamma, A \vdash C}}{\Gamma \vdash C} \; \wedge\text{-e1}$$

reduces to $(\pi_1/A)\pi_3$, that is the proof π_3 where the use of the rule axiom with the proposition A has been replaced with the proof π_1. And, similarly, the proof

$$\frac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B} \; \wedge\text{-i} \quad \dfrac{\pi_3}{\Gamma, B \vdash C}}{\Gamma \vdash C} \; \wedge\text{-e2}$$

reduces to $(\pi_2/B)\pi_3$.

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

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

require A or B and to prove a proposition C, the elimination rule of the disjunction

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

provides A or B and a proof reduction process can be defined in a similar way.

The property that the elimination rules provide exactly the propositions required by the introduction rules can be split into two properties, that it provides no more and no less (called "harmony" and "reversed harmony" in [10]).

We can also imagine deduction rules that do not verify this inversion principle, either because the elimination rules provide propositions not required by the introduction rules, or because the introduction rules require propositions not provided by the elimination rules, or both. When the propositions provided by the elimination rules are not all required by the introduction rules, we call the deduction rules *insufficient*. When the propositions provided by the eliminations rule are required by the introductions rule, but some propositions required by the introduction rules are not provided by the elimination rules, we call them *excessive*.

An example of a connective with insufficient deduction rules is Prior's *tonk* [18] whose introduction rule

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

requires A and whose elimination rule

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

provides B. Thus, the proposition B is provided by the elimination rule, but not required by the introduction rule. Because of this insufficiency, the proof

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

cannot be reduced. An example of a connective with excessive deduction rules is the connective $\frown$ that is similar to the conjunction, except that the second elimination rule has been dropped. Thus, its introduction rule

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

requires A and B, but its elimination rule

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

provides A only. Thus the proposition B is required by the introduction rules, but not provided by the elimination rules. For such connectives, a proof reduction process can still be defined, for example the proof

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

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

Another example is the connective $\odot$ whose introduction rule

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

similar to that of the conjunction, requires A and B and whose elimination rule

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

similar to that of the disjunction, provides A or B. In this case also, proofs can be reduced. Moreover, several proof reduction processes can be defined, exploiting, in different ways, the excess of the deduction rules. For example, the proof

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

can be reduced to $(\pi_1/A)\pi_3$, it can be reduced to $(\pi_2/B)\pi_4$, it also can be reduced, in a non-deterministic way, either to $(\pi_1/A)\pi_3$ or to $(\pi_2/B)\pi_4$.

A final example is the quantifier $\nexists$, whose introduction rule

$$\frac{\Gamma \vdash A}{\Gamma \vdash \nexists x \ A} \ \nexists\text{-i} \ x \text{ not free in } \Gamma$$

3

similar to that of the universal quantifier, requires a proof of A for all x and whose elimination rule

$$\frac{\Gamma \vdash \not\exists x\ A \quad \Gamma, A \vdash C}{\Gamma \vdash C} \ \not\exists\text{-e } x \text{ not free in } \Gamma, C$$

similar to that of the existential quantifier, provides a proof of A for some x. The proof

$$\frac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A}}{\Gamma \vdash \not\exists x\ A}\ \not\exists\text{-i} \quad \dfrac{\pi_2}{\Gamma, A \vdash C}}{\Gamma \vdash C}\ \not\exists\text{-e}$$

can be reduced, in a non-deterministic way, to $((t/x)\pi_1/A)(t/x)\pi_2$, for any term t.

The quantifier ∇ [14], defined in sequent calculus rather than natural deduction, may also be considered as a quantifier with excessive deduction rules, 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, which we do not address here.

1.2. Mixing excessiveness and harmony

The rules

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

are excessive.

But, we can add another set of elimination rules for the connective $\odot$, similar to those of conjunction

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

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

Then, the connective $\odot$, with its four rules $\odot$-i, $\odot$-e, $\odot$-e1, and $\odot$-e2, appears as a two-face connective: the subset of its deduction rules $\{\odot\text{-i}, \odot\text{-e}\}$ is excessive, while the subset $\{\odot\text{-i}, \odot\text{-e1}, \odot\text{-e2}\}$ is harmonious. Note that the rules $\{\odot\text{-i}, \odot\text{-e1}, \odot\text{-e2}\}$ are exactly those of the conjunction.

1.3. Information loss

We say that an occurrence of a sub-proof π_1 of a proof π is *accessible*, if there exists a context κ such that $\kappa\{\pi_X\}$, where π_X is obtained by replacing this occurrence of π_1 with a variable X, reduces to X.

For example, the occurrence of π_1 in the proof

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

is accessible, as putting the proof

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

in the context

$$\frac{\dfrac{\{\}}{\Gamma \vdash A \wedge B} \quad \dfrac{}{\Gamma, A \vdash A}\ \text{axiom}}{\Gamma \vdash A}\ \wedge\text{-e1}$$

yields the proof

$$\dfrac{\dfrac{\dfrac{X}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B} \wedge\text{-i} \quad \dfrac{}{\Gamma, A \vdash A} \text{axiom}}{\Gamma \vdash A} \wedge\text{-e1}$$

that reduces to X. In other words, the rule $\wedge$-i puts the proofs π_1 and π_2 in a box, but the box can be opened and the proofs can be taken out of it.

With harmonious deduction rules, when a proof is built with an introduction rule, the proofs of its premises remain accessible. The situation is different with excessive deduction rules: 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 occurrence of π_2 in the proof

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

is inaccessible as there is no context such that putting the proof

$$\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{X}{\Gamma \vdash B}}{\Gamma \vdash A \frown B} \frown\text{-i}$$

in that context yields a proof that reduces to X. Again, the rule $\frown$-i puts the proofs π_1 and π_2 in a box, the box can be partially opened and the proof π_1 can be taken out of it, but not the proof π_2, that is inaccessible. The information it contains is lost.

The accessibility of the occurrences of π_1 and π_2 of the proof

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

depends on the elimination rules we allow in the context and on the way we 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 allow the rule $\odot$-e in the context, but neither $\odot$-e1 nor $\odot$-e2, and reduce this proof systematically to $(\pi_1/A)\pi_3$, then π_1 is accessible, but π_2 is not. If we reduce it systematically to $(\pi_2/B)\pi_4$, then π_2 is accessible, but π_1 is not. If we reduce it, in a non-deterministic way, to $(\pi_1/A)\pi_3$ or to $(\pi_2/B)\pi_4$, then both π_1 and π_2 are accessible, but in a non-deterministic way. If we allow the rule $\odot$-e1 and $\odot$-e2 in the context, then both proofs are accessible. Once more, the rule $\odot$-i puts the proofs π_1 and π_2 in a box, whether the box can be opened and the proofs taken out of it, depends on the tools we use to open it.

When a connective has non-harmonious deduction rules, its introduction rules alone do not define its meaning, 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 a connective.

While connectives with harmonious deduction rules model information-preservation, reversibility, and determinism, those with excessive deduction rules model information-erasure, non-reversibility, and non-determinism. In particular, the elimination rules $\odot$-e1 and $\odot$-e2 will be used to model information-preservation, reversibility, and determinism, while the elimination rule $\odot$-e will be used to 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.

Several programming languages have been proposed to express quantum algorithms, for example [1, 23, 25, 2, 3, 7, 5]. The design of such quantum programming languages raises two main questions. The first is to take into account the linearity of the unitary operators and, for instance, avoid cloning, and the second is to express the information-erasure, non-reversibility, and non-determinism of the measurement. 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 $\odot$-e (Section 4.5).

In previous works, we have attempted to formalize superposition and measurement in the λ-calculus. The calculus Lambda-$\mathcal{S}$ [7] contains a primitive constructor $+$ and a primitive measurement symbol π, together with a rule reducing $\pi(t + u)$, in a non-deterministic way, to t or to u.

The superposition $t + u$ can also be considered as the pair $\langle t, u \rangle$. Hence, it should have the type $A \wedge A$. In other words, it should be a proof of the proposition $A \wedge A$. In System I [4], various type-isomorphisms have been taken as identities, 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 parameterized 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, in a non-deterministic way, to t or to u, 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, it should be the connective $\odot$.

In this paper, we present a propositional logic with the connective $\odot$ and two interstitial rules, a language of proof-terms for this logic, the $\odot$-calculus (read: "the sup-calculus"), and we prove the termination of proof-reduction (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. A vector $\binom{a}{b}$ will be expressed as the proof $[a.\star, b.\star]$ of $\top \odot \top$, where $\star$ is the symbol corresponding to the introduction rule of $\top$, $[,]$ that of $\odot$, and a and b are scalars.

Propositional logic with $\odot$ is not a logic to reason about quantum programs, but its propositions can be seen as types of quantum programs.

A preliminary version of this paper has been published in the proceedings of the *International Colloquium on Theoretical Aspects of Computing*, 2021. In this journal version, we have replaced the symbol $\delta_\odot^\parallel$ with the symbols $\delta_\odot^1$, $\delta_\odot^2$, clarifying the two-face nature of the connective $\odot$. We have also introduced an elimination rule for the symbol $\top$. Such a rule is often considered as redundant, but it fully makes sense in natural deduction with generalized elimination rules, and even more in a proof system with scalars, such as that of Section 3. Besides providing the complete proofs of all theorems, we investigate, in this paper, the confluence of the deterministic part of the calculus, that was not addressed in the conference version. To our surprise, the system without scalars was confluent, but the system with scalars was not. This led us to modify the treatment of scalars and the definition of matrices to make this system confluent. Finally, the conference version of the paper only addressed quantum algorithms on one and two qubits. In this version, we have generalized this to arbitrary quantum algorithms, leading to a more systematic treatment of vectors, matrices, and measurement.

$$\frac{}{\Gamma \vdash A} \text{ axiom } A \in \Gamma \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash A}{\Gamma \vdash A} \text{ sum} \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A} \text{ prod}$$

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

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

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

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

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

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

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

2. Propositional logic with $\odot$

We consider a constructive propositional logic with the usual connectives $\top$, $\bot$, $\Rightarrow$, $\wedge$, and $\vee$ (as usual, negation is defined as $\neg A = (A \Rightarrow \bot)$), and the extra connective $\odot$. 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 in Figure 1.

The rules axiom, $\top$-i, $\top$-e, $\bot$-e, $\Rightarrow$-i, $\Rightarrow$-e, $\wedge$-i, $\wedge$-e1, $\wedge$-e2, $\vee$-i1, $\vee$-i2, and $\vee$-e are the usual rules of constructive propositional logic. The rules $\odot$-i, $\odot$-e, $\odot$-e1, and $\odot$-e2 are those of the connective $\odot$. We also added two interstitial rules

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

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

whose premises are identical to their conclusion. Although these rules are logically trivial, they introduce constructors in the proof language that will be of key importance when we extend the calculus with scalars, in Section 3. Their names will also be explained there.

2.1. Proof reduction

Reducible expressions (redexes) in this logic are the usual ones for the connectives $\Rightarrow$, $\wedge$, $\vee$, and $\top$

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

$$\frac{\dfrac{\begin{array}{c}\pi_1\\\Gamma \vdash A\end{array} \quad \begin{array}{c}\pi_2\\\Gamma \vdash B\end{array}}{\Gamma \vdash A \wedge B} \wedge\text{-i} \quad \begin{array}{c}\pi_3\\\Gamma, A \vdash C\end{array}}{\Gamma \vdash C} \wedge\text{-e1} \qquad \text{that reduces to} \qquad (\pi_1/A)\pi_3$$

$$\frac{\dfrac{\begin{array}{c}\pi_1\\\Gamma \vdash A\end{array} \quad \begin{array}{c}\pi_2\\\Gamma \vdash B\end{array}}{\Gamma \vdash A \wedge B} \wedge\text{-i} \quad \begin{array}{c}\pi_3\\\Gamma, B \vdash C\end{array}}{\Gamma \vdash C} \wedge\text{-e2} \qquad \text{that reduces to} \qquad (\pi_2/B)\pi_3$$

7

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

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

and

$$\dfrac{\dfrac{}{\Gamma \vdash \top}\ \top\text{-i} \quad \dfrac{\pi}{\Gamma \vdash C}}{\Gamma \vdash C}\ \top\text{-e} \qquad \text{that reduces to} \qquad \dfrac{\dfrac{\pi}{\Gamma \vdash C}}{\Gamma \vdash C}\ \text{prod}$$

that is to π with an added interstitial rule, and the redexes for the connective $\odot$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \odot B}\ \odot\text{-i} \quad \dfrac{\pi_3}{\Gamma, A \vdash C} \quad \dfrac{\pi_4}{\Gamma, B \vdash C}}{\Gamma \vdash C}\ \odot\text{-e} \qquad \text{that reduces to} \qquad (\pi_1/A)\pi_3 \text{ and } (\pi_2/B)\pi_4$$

in a non-deterministic way, erasing some information

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \odot B}\ \odot\text{-i} \quad \dfrac{\pi_3}{\Gamma, A \vdash C}}{\Gamma \vdash C}\ \odot\text{-e1} \qquad \text{that reduces to} \qquad (\pi_1/A)\pi_3$$

and

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \odot B}\ \odot\text{-i} \quad \dfrac{\pi_3}{\Gamma, B \vdash C}}{\Gamma \vdash C}\ \odot\text{-e2} \qquad \text{that reduces to} \qquad (\pi_2/A)\pi_3$$

Adding the interstitial rules, permits to build proofs that cannot be reduced, because the introduction rule of some connective and its elimination rule are separated by the rule sum or the rule prod, for example

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\ \wedge\text{-i} \quad \dfrac{\dfrac{\pi_3}{\Gamma \vdash A} \quad \dfrac{\pi_4}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\ \wedge\text{-i}}{\Gamma \vdash A \wedge B}\ \text{sum} \quad \dfrac{\pi_5}{\Gamma, A \vdash C}}{\Gamma \vdash C}\ \wedge\text{-e1}$$

Reducing such a proof requires rules to commute the rule sum 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

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

the commutation with the elimination rule below is often preferred. In this paper, we favor the commutation of the interstitial rules 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

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

reduces to

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

Such a commutation yields a stronger introduction property for the considered connective (Theorem 2.30).

In the proof

$$\cfrac{\cfrac{\cfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash A \vee B}\text{ }\vee\text{-i1}}{\Gamma \vdash A \vee B}\text{ prod}$$

the prod rule and the $\vee$-i1 rule can be commuted. For coherence, we have decided to commute both the sum rule and the prod rule with the elimination rule of the disjunction, rather that with its introduction rules, but both choices are possible.

2.2. Proof-terms

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

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

The variables x express the proofs built with the rule axiom, the terms $t \text{\textbf{+}} u$ those built with the rule sum, the terms $\bullet t$ those built with the rule prod, the term $\star$ that built with the rule $\top$-i, the terms $\delta_\top(t, u)$ those built with the rule $\top$-e, the terms $\delta_\bot(t)$ those built with the rule $\bot$-e, the terms $\lambda x.t$ those built with the rule $\Rightarrow$-i, the terms $t\ u$ those built with the rule $\Rightarrow$-e, the terms $\langle t, u \rangle$ those built with the rule $\wedge$-i, the terms $\delta_\wedge^1(t, x.u)$ and $\delta_\wedge^2(t, x.u)$ those built with the rules $\wedge$-e1 and $\wedge$-e2, the terms $inl(t)$ and $inr(t)$ those built with the rules $\vee$-i1 and $\vee$-i2, the terms $\delta_\vee(t, x.u, y.v)$ those built with the rule $\vee$-e, the terms $[t, u]$ those built with the rule $\odot$-i, and the terms $\delta_\odot(t, x.u, y.v)$, $\delta_\odot^1(t, x.u)$, and $\delta_\odot^2(t, x.u)$ those built with the rules $\odot$-e, $\odot$-e1, and $\odot$-e2.

The proofs of the form $\star$, $\lambda x.t$, $\langle t, u \rangle$, $inl(t)$, $inr(t)$, and $[t, u]$ are called *introductions*, and those of the form $\delta_\top(t, u)$, $\delta_\bot(t)$, $t\ u$, $\delta_\wedge^1(t, x.u)$, $\delta_\wedge^2(t, x.u)$, $\delta_\vee(t, x.u, y.v)$, $\delta_\odot(t, x.u, y.v)$, $\delta_\odot^1(t, x.u)$, and $\delta_\odot^2(t, x.u)$ *eliminations*. The variables and the proofs of the form $t \text{\textbf{+}} u$ and $\bullet t$ are neither introductions nor eliminations.

The α-equivalence relation and the free and bound variables of a proof-term are defined as usual. Proof-terms are defined modulo α-equivalence. A proof-term is closed if it contains no free variables. We write $(u/x)t$ for the substitution of u for x in t.

The typing rules of the $\odot$-calculus are given in Figure 2 and its reduction rules in Figure 3. An instance of the second rule of Figure 3 is

$$(\lambda x.x)\ y \longrightarrow y$$

and an instance of the third is

$$\delta_\wedge^1(\langle \star, \star \rangle, x.x) \longrightarrow \star$$

Remark 2.1. *This system is a higher-order rewrite system [11, 12]. A more rigorous notation would be to consider the symbol . as the abstraction, to add a symbol app for application, and to add a rewrite rule β, $app(x.t, u) \longrightarrow (u/x)t$ used to build the instances of the rules.*

Hence, the second rule of Figure 3 would be expressed as

$$(\lambda x.app(T, x))\ U \longrightarrow app(T, U)$$

the third as

$$\delta_\wedge^1(\langle T, U \rangle, x.app(V, x)) \longrightarrow app(V, T)$$

9

$$\frac{}{\Gamma \vdash x : A} \; \text{axiom } x : A \in \Gamma \qquad \frac{\Gamma \vdash t : A \quad \Gamma \vdash u : A}{\Gamma \vdash t + u : A} \; \text{sum} \qquad \frac{\Gamma \vdash t : A}{\Gamma \vdash \bullet t : A} \; \text{prod}$$

$$\frac{}{\Gamma \vdash \star : \top} \; \top\text{-i} \qquad \frac{\Gamma \vdash t : \top \quad \Gamma \vdash u : C}{\Gamma \vdash \delta_\top(t, u) : C} \; \top\text{-e} \qquad \frac{\Gamma \vdash t : \bot}{\Gamma \vdash \delta_\bot(t) : C} \; \bot\text{-e}$$

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

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash u : B}{\Gamma \vdash \langle t, u \rangle : A \wedge B} \; {\wedge}\text{-i}$$

$$\frac{\Gamma \vdash t : A \wedge B \quad \Gamma, x : A \vdash u : C}{\Gamma \vdash \delta_\wedge^1(t, x.u) : C} \; {\wedge}\text{-e1} \qquad \frac{\Gamma \vdash t : A \wedge B \quad \Gamma, x : B \vdash u : C}{\Gamma \vdash \delta_\wedge^2(t, x.u) : C} \; {\wedge}\text{-e2}$$

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

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

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash u : B}{\Gamma \vdash [t, u] : A \odot B} \; {\odot}\text{-i}$$

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

$$\frac{\Gamma \vdash t : A \odot B \quad \Gamma, x : A \vdash u : C}{\Gamma \vdash \delta_\odot^1(t, x.u) : C} \; {\odot}\text{-e1} \qquad \frac{\Gamma \vdash t : A \odot B \quad \Gamma, x : B \vdash u : C}{\Gamma \vdash \delta_\odot^2(t, x.u) : C} \; {\odot}\text{-e2}$$

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

etc.

Substituting the proof $x.x$ for the variable T and the proof y for the variable U in the first rule and reducing, with the added rule, both sides of the rule yields the instance

$$(\lambda x.x) \; y \longrightarrow y$$

and substituting $\star$ for the variables T and U and the proof $x.x$ for the variable V, in the second, and reducing both sides of the rule, with the added rule, yields the instance

$$\delta_\wedge^1(\langle \star, \star \rangle, x.x) \longrightarrow \star$$

etc.

2.3. Subject reduction

To prove subject reduction, we first prove, as usual, a substitution lemma.

Proposition 2.2 (Substitution). *If $\Gamma, x : B \vdash t : A$ and $\Gamma \vdash u : B$, then $\Gamma \vdash (u/x)t : A$.*

Proof. By induction on the structure of t. $\qquad \square$

And use this lemma to prove the theorem itself.

Theorem 2.3 (Subject reduction). *If $\Gamma \vdash t : A$ and $t \longrightarrow u$, then $\Gamma \vdash u : A$.*

Proof. By induction on the definition of the relation $\longrightarrow$. $\qquad \square$

$$\delta_\top(\star, t) \longrightarrow \bullet t$$
$$(\lambda x.t)\ u \longrightarrow (u/x)t$$
$$\delta_\wedge^1(\langle t, u \rangle, x.v) \longrightarrow (t/x)v$$
$$\delta_\wedge^2(\langle t, u \rangle, x.v) \longrightarrow (u/x)v$$
$$\delta_\vee(inl(t), x.v, y.w) \longrightarrow (t/x)v$$
$$\delta_\vee(inr(u), x.v, y.w) \longrightarrow (u/y)w$$
$$\delta_\odot([t, u], x.v, y.w) \longrightarrow (t/x)v$$
$$\delta_\odot([t, u], x.v, y.w) \longrightarrow (u/y)w$$
$$\delta_\odot^1([t, u], x.v) \longrightarrow (t/x)v$$
$$\delta_\odot^2([t, u], x.v) \longrightarrow (u/x)v$$

$$\star + \star \longrightarrow \star$$
$$(\lambda x.t) + (\lambda x.u) \longrightarrow \lambda x.(t + u)$$
$$\langle t, u \rangle + \langle v, w \rangle \longrightarrow \langle t + v, u + w \rangle$$
$$\delta_\vee(t + u, x.v, y.w) \longrightarrow \delta_\vee(t, x.v, y.w) + \delta_\vee(u, x.v, y.w)$$
$$[t, u] + [v, w] \longrightarrow [t + v, u + w]$$

$$\bullet\star \longrightarrow \star$$
$$\bullet(\lambda x.t) \longrightarrow \lambda x.(\bullet t)$$
$$\bullet\langle t, u \rangle \longrightarrow \langle \bullet t, \bullet u \rangle$$
$$\delta_\vee(\bullet t, x.v, y.w) \longrightarrow \bullet\delta_\vee(t, x.v, y.w)$$
$$\bullet[t, u] \longrightarrow [\bullet t, \bullet u]$$

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

2.4. Confluence

The system presented in Figure 3 is trivially non-confluent, because of the non-deterministic rules

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

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

But if we drop these two rules, the rest of the system is confluent.

Theorem 2.4. *The system of Figure 3 without the rules*

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

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

is confluent.

Proof. This system is left linear and it has no critical pairs. As proved in [12, Theorem 6.8], higher-order left linear systems without critical pairs are confluent. □

Note that the untyped calculus does have critical pairs, for example the proof $\delta_\vee(\star + \star, x.x, y.y)$ reduces in two different ways, but these critical pairs are not well-typed.

2.5. Termination

We now prove the strong termination of proof reduction, that is that all reduction sequences are finite. The proof follows the same pattern as that for propositional natural deduction, that we recall in the Appendix.

The $\odot$-calculus introduces two new features: the connective $\odot$, its associated proof constructors $[,], \delta_\odot$, $\delta_\odot^1$, and $\delta_\odot^2$, and the constructors $+$ and $\bullet$. The termination proof of propositional natural deduction extends

11

smoothly when we add the connective $\odot$, but adding the constructors $\boldsymbol{+}$ and $\bullet$ is a bit more challenging. To handle these symbols, we prove the strong termination of an extended reduction system, in the spirit of Girard's ultra-reduction [9], whose strong termination obviously implies that of the rules of Figure 3.

Definition 2.5 (Ultra-reduction). *Ultra-reduction is defined with the rules of Figure 3, plus the rules*

$$t \boldsymbol{+} u \longrightarrow t$$
$$t \boldsymbol{+} u \longrightarrow u$$
$$\bullet t \longrightarrow t$$

In the proof below, Propositions 2.8, 2.11, 2.12, 2.13, 2.14, 2.15, 2.20, 2.21, 2.22, and 2.23 have the same proofs as Propositions Appendix A.6, Appendix A.9, Appendix A.10, Appendix A.11, Appendix A.12, Appendix A.13, Appendix A.15, Appendix A.16, Appendix A.17, and Appendix A.18 in the strong termination of proof reduction for propositional natural deduction (except that the references to Propositions Appendix A.6, Appendix A.7, and Appendix A.8 must be replaced with references to Propositions 2.8, 2.9, and 2.10). So we will omit these proofs. Propositions 2.9, 2.10, 2.19, and 2.24 have proofs similar to those of Propositions Appendix A.7, Appendix A.8, Appendix A.14, and Appendix A.19, but these proofs require minor tweaks. In contrast, Propositions 2.16, 2.17, 2.18, 2.25, 2.26, and 2.27 are specific.

Definition 2.6. *We define, by induction on the proposition A, a set of proofs $[\![A]\!]$:*

- $t \in [\![\top]\!]$ *if t strongly terminates,*

- $t \in [\![\bot]\!]$ *if t strongly terminates,*

- $t \in [\![A \Rightarrow B]\!]$ *if t strongly terminates and whenever it reduces to a proof of the form $\lambda x.u$, then for every $v \in [\![A]\!]$, $(v/x)u \in [\![B]\!]$,*

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

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

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

Definition 2.7. *If t is a strongly terminating proof, we write $|t|$ for the maximum length of a reduction sequence issued from t.*

Proposition 2.8 (Variables). *For any A, the set $[\![A]\!]$ contains all the variables.*

Proposition 2.9 (Closure by reduction). *If $t \in [\![A]\!]$ and $t \longrightarrow^* t'$, then $t' \in [\![A]\!]$.*

Proof. If $t \longrightarrow^* t'$ and t strongly terminates, then t' strongly terminates.

Furthermore, if A has the form $B \Rightarrow C$ and t' reduces to $\lambda x.u$, then so does t, hence for every $v \in [\![B]\!]$, $(v/x)u \in [\![C]\!]$.

If A has the form $B \wedge C$ and t' reduces to $\langle u, v \rangle$, then so does t, hence $u \in [\![B]\!]$ and $v \in [\![C]\!]$.

If A has the form $B \vee C$ and t' reduces to $inl(u)$, then so does t, hence $u \in [\![B]\!]$ and if A has the form $B \vee C$ and t' reduces to $inr(v)$, then so does t, hence $v \in [\![C]\!]$.

And if A has the form $B \odot C$ and t' reduces to $[u, v]$, then so does t, hence $u \in [\![B]\!]$ and $v \in [\![C]\!]$. $\qquad\square$

Proposition 2.10 (Girard's lemma). *Let t be a proof that is not an introduction, such that all the one-step reducts of t are in $[\![A]\!]$. Then $t \in [\![A]\!]$.*

Proof. Let $t, t_2, ...$ be a reduction sequence issued from t. If it has a single element, it is finite. Otherwise, we have $t \longrightarrow t_2$. As $t_2 \in [\![A]\!]$, it strongly terminates and the reduction sequence is finite. Thus, t strongly terminates.

Furthermore, if A has the form $B \Rightarrow C$ and $t \longrightarrow^* \lambda x.u$, then let $t, t_2, ..., t_n$ be a reduction sequence from t to $\lambda x.u$. As t_n is an introduction and t is not, $n \geq 2$. Thus, $t \longrightarrow t_2 \longrightarrow^* t_n$. We have $t_2 \in [\![A]\!]$, thus for all $v \in [\![B]\!]$, $(v/x)u \in [\![C]\!]$.

And if A has the form $B \wedge C$ and $t \longrightarrow^* \langle u, v \rangle$, then let $t, t_2, ..., t_n$ be a reduction sequence from t to $\langle u, v \rangle$. As t_n is an introduction and t is not, $n \geq 2$. Thus, $t \longrightarrow t_2 \longrightarrow^* t_n$. We have $t_2 \in [\![A]\!]$, thus $u \in [\![B]\!]$ and $v \in [\![C]\!]$.

If A has the form $B \vee C$ and $t \longrightarrow^* inl(u)$, then let $t, t_2, ..., t_n$ be a reduction sequence from t to $inl(u)$. As t_n is an introduction and t is not, $n \geq 2$. Thus, $t \longrightarrow t_2 \longrightarrow^* t_n$. We have $t_2 \in [\![A]\!]$, thus $u \in [\![B]\!]$.

If A has the form $B \vee C$ and $t \longrightarrow^* inr(v)$, then let $t, t_2, ..., t_n$ be a reduction sequence from t to $inr(v)$. As t_n is an introduction and t is not, $n \geq 2$. Thus, $t \longrightarrow t_2 \longrightarrow^* t_n$. We have $t_2 \in [\![A]\!]$, thus $v \in [\![C]\!]$.

And if A has the form $B \odot C$ and $t \longrightarrow^* [u, v]$, then let $t, t_2, ..., t_n$ be a reduction sequence from t to $[u, v]$. As t_n is an introduction and t is not, $n \geq 2$. Thus, $t \longrightarrow t_2 \longrightarrow^* t_n$. We have $t_2 \in [\![A]\!]$, thus $u \in [\![B]\!]$ and $v \in [\![C]\!]$. $\square$

In Propositions 2.11 to 2.27, we prove the adequacy of each proof constructor.

Proposition 2.11 (Adequacy of $\star$). *We have $\star \in [\![\top]\!]$.*

Proposition 2.12 (Adequacy of λ). *If, for all $u \in [\![A]\!]$, $(u/x)t \in [\![B]\!]$, then $\lambda x.t \in [\![A \Rightarrow B]\!]$.*

Proposition 2.13 (Adequacy of $\langle, \rangle$). *If $t_1 \in [\![A]\!]$ and $t_2 \in [\![B]\!]$, then $\langle t_1, t_2 \rangle \in [\![A \wedge B]\!]$.*

Proposition 2.14 (Adequacy of inl). *If $t \in [\![A]\!]$, then $inl(t) \in [\![A \vee B]\!]$.*

Proposition 2.15 (Adequacy of inr). *If $t \in [\![B]\!]$, then $inr(t) \in [\![A \vee B]\!]$.*

Proposition 2.16 (Adequacy of $[,]$). *If $t_1 \in [\![A]\!]$ and $t_2 \in [\![B]\!]$, then $[t_1, t_2] \in [\![A \odot B]\!]$.*

Proof. The proofs t_1 and t_2 strongly terminate. Consider a reduction sequence issued from $[t_1, t_2]$. This sequence can only reduce t_1 and t_2, hence it is finite. Thus, $[t_1, t_2]$ strongly terminates.

Furthermore, if $[t_1, t_2] \longrightarrow^* [t_1', t_2']$, then $t_1' \longrightarrow^* t_1$ and $t_2' \longrightarrow^* t_2$. By Proposition 2.9, $t_1' \in [\![A]\!]$ and $t_2' \in [\![B]\!]$. $\square$

Proposition 2.17 (Adequacy of $+$). *If $t_1 \in [\![A]\!]$ and $t_2 \in [\![A]\!]$, then $t_1 + t_2 \in [\![A]\!]$.*

Proof. The proofs t_1 and t_2 strongly terminate. We prove, by induction on the structure of A and then on $|t_1| + |t_2|$, that $t_1 + t_2 \in [\![A]\!]$. Using Proposition 2.10, we only need to prove that every of its one step reducts is in $[\![A]\!]$. If the reduction takes place in t_1 or in t_2, then we apply Proposition 2.9 and the induction hypothesis. Otherwise, either:

- The proofs t_1 and t_2 are equal to $\star$ and the reduct is $\star$ that is in $[\![A]\!]$.

- The proposition A has the form $B \Rightarrow C$, $t_1 = \lambda x.u_1$, $t_2 = \lambda x.u_2$, and the reduct is $\lambda x.(u_1 + u_2)$. As $t_1 = \lambda x.u_1 \in [\![A]\!] = [\![B \Rightarrow C]\!]$, for every w in $[\![B]\!]$, $(w/x)u_1 \in [\![C]\!]$. In a similar way, $(w/x)u_2 \in [\![C]\!]$. By induction hypothesis, $(w/x)(u_1 + u_2) = (w/x)u_1 + (w/x)u_2 \in [\![C]\!]$ and by Proposition 2.12, $\lambda x.(u_1 + u_2) \in [\![B \Rightarrow C]\!] = [\![A]\!]$.

- The proposition A has the form $B \wedge C$, $t_1 = \langle u_1, v_1 \rangle$, $t_2 = \langle u_2, v_2 \rangle$, and the reduct is $\langle u_1 + u_2, v_1 + v_2 \rangle$. As $t_1 = \langle u_1, v_1 \rangle \in [\![A]\!] = [\![B \wedge C]\!]$, $u_1 \in [\![B]\!]$ and $v_1 \in [\![C]\!]$. In a similar way, $u_2 \in [\![B]\!]$ and $v_2 \in [\![C]\!]$. By induction hypothesis, $u_1 + u_2 \in [\![B]\!]$ and $v_1 + v_2 \in [\![C]\!]$ and by Proposition 2.13, $\langle u_1 + u_2, v_1 + v_2 \rangle \in [\![B \wedge C]\!] = [\![A]\!]$.

13

- The proposition A has the form $B \odot C$, $t_1 = [u_1, v_1]$, $t_2 = [u_2, v_2]$, and the reduct is $[u_1 + u_2, v_1 + v_2]$. As $t_1 = [u_1, v_1] \in \llbracket A \rrbracket = \llbracket B \odot C \rrbracket$, $u_1 \in \llbracket B \rrbracket$ and $v_1 \in \llbracket C \rrbracket$. In a similar way, $u_2 \in \llbracket B \rrbracket$ and $v_2 \in \llbracket C \rrbracket$. By induction hypothesis, $u_1 + u_2 \in \llbracket B \rrbracket$ and $v_1 + v_2 \in \llbracket C \rrbracket$ and by Proposition 2.16, $[u_1 + u_2, v_1 + v_2] \in \llbracket B \odot C \rrbracket = \llbracket A \rrbracket$.

- The reduction rule is an ultra-reduction rule and the reduct is t_1 or t_2, that are in $\llbracket A \rrbracket$. $\qquad\square$

Proposition 2.18 (Adequacy of $\bullet$)**.** *If* $t \in \llbracket A \rrbracket$, *then* $\bullet t \in \llbracket A \rrbracket$.

Proof. The proof t strongly terminates. We prove, by induction on the structure of A and then on $|t|$, that $\bullet t \in \llbracket A \rrbracket$. Using Proposition 2.10, we only need to prove that every of its one step reducts is in $\llbracket A \rrbracket$. If the reduction takes place in t, then we apply Proposition 2.9 and the induction hypothesis. Otherwise, either:

- The proof t is equal to $\star$ and the reduct is $\star$ that is in $\llbracket A \rrbracket$.

- The proposition A has the form $B \Rightarrow C$, $t = \lambda x.u$, and the reduct is $\lambda x. \bullet u$. As $t = \lambda x.u \in \llbracket A \rrbracket = \llbracket B \Rightarrow C \rrbracket$, for every w in $\llbracket B \rrbracket$, $(w/x)u \in \llbracket C \rrbracket$. By induction hypothesis, $(w/x) \bullet u = \bullet(w/x)u \in \llbracket C \rrbracket$ and by Proposition 2.12, $\lambda x. \bullet u \in \llbracket B \Rightarrow C \rrbracket = \llbracket A \rrbracket$.

- The proposition A has the form $B \wedge C$, $t = \langle u, v \rangle$ and the reduct is $\langle \bullet u, \bullet v \rangle$. As $t = \langle u, v \rangle \in \llbracket A \rrbracket = \llbracket B \wedge C \rrbracket$, $u \in \llbracket B \rrbracket$ and $v \in \llbracket C \rrbracket$. By induction hypothesis, $\bullet u \in \llbracket B \rrbracket$ and $\bullet v \in \llbracket C \rrbracket$ and by Proposition 2.13, $\langle \bullet u, \bullet v \rangle \in \llbracket B \wedge C \rrbracket = \llbracket A \rrbracket$.

- The proposition A has the form $B \odot C$, $t = [u, v]$ and the reduct is $[\bullet u, \bullet v]$. As $t = [u, v] \in \llbracket A \rrbracket = \llbracket B \odot C \rrbracket$, $u \in \llbracket B \rrbracket$ and $v \in \llbracket C \rrbracket$. By induction hypothesis, $\bullet u \in \llbracket B \rrbracket$ and $\bullet v \in \llbracket C \rrbracket$ and by Proposition 2.16, $[\bullet u, \bullet v] \in \llbracket B \odot C \rrbracket = \llbracket A \rrbracket$.

- The reduction rule is an ultra-reduction rule and the reduct is t, that is in $\llbracket A \rrbracket$. $\qquad\square$

Proposition 2.19 (Adequacy of $\delta_\top$)**.** *If* $t_1 \in \llbracket \top \rrbracket$ *and* $t_2 \in \llbracket C \rrbracket$, *then* $\delta_\top(t_1, t_2) \in \llbracket C \rrbracket$.

Proof. The proofs t_1 and t_2 strongly terminate. We prove, by induction on $|t_1| + |t_2|$, that $\delta_\top(t_1, t_2) \in \llbracket C \rrbracket$. Using Proposition 2.10, we only need to prove that every of its one step reducts is in $\llbracket C \rrbracket$. If the reduction takes place in t_1 or t_2, then we apply Proposition 2.9 and the induction hypothesis.

Otherwise, the proof t_1 is $\star$ and the reduct is $\bullet t_2$. We conclude with Proposition 2.18. $\qquad\square$

Proposition 2.20 (Adequacy of $\delta_\perp$)**.** *If* $t \in \llbracket \perp \rrbracket$, *then* $\delta_\perp(t) \in \llbracket C \rrbracket$.

Proposition 2.21 (Adequacy of application)**.** *If* $t_1 \in \llbracket A \Rightarrow B \rrbracket$ *and* $t_2 \in \llbracket A \rrbracket$, *then* $t_1\ t_2 \in \llbracket B \rrbracket$.

Proposition 2.22 (Adequacy of $\delta_\wedge^1$)**.** *If* $t_1 \in \llbracket A \wedge B \rrbracket$ *and, for all* u *in* $\llbracket A \rrbracket$, $(u/x)t_2 \in \llbracket C \rrbracket$, *then* $\delta_\wedge^1(t_1, x.t_2) \in \llbracket C \rrbracket$.

Proposition 2.23 (Adequacy of $\delta_\wedge^2$)**.** *If* $t_1 \in \llbracket A \wedge B \rrbracket$ *and, for all* u *in* $\llbracket B \rrbracket$, $(u/x)t_2 \in \llbracket C \rrbracket$, *then* $\delta_\wedge^2(t_1, x.t_2) \in \llbracket C \rrbracket$.

Proposition 2.24 (Adequacy of $\delta_\vee$)**.** *If* $t_1 \in \llbracket A \vee B \rrbracket$, *for all* u *in* $\llbracket A \rrbracket$, $(u/x)t_2 \in \llbracket C \rrbracket$, *and, for all* v *in* $\llbracket B \rrbracket$, $(v/y)t_3 \in \llbracket C \rrbracket$, *then* $\delta_\vee(t_1, x.t_2, y.t_3) \in \llbracket C \rrbracket$.

Proof. By Proposition 2.8, $x \in \llbracket A \rrbracket$, thus $t_2 = (x/x)t_2 \in \llbracket C \rrbracket$. In the same way, $t_3 \in \llbracket C \rrbracket$. Hence, t_1, t_2, and t_3 strongly terminate. We prove, by induction on $|t_1| + |t_2| + |t_3|$, that $\delta_\vee(t_1, x.t_2, y.t_3) \in \llbracket C \rrbracket$. Using Proposition 2.10, we only need to prove that every of its one step reducts is in $\llbracket C \rrbracket$. If the reduction takes place in t_1, t_2, or t_3, then we apply Proposition 2.9 and the induction hypothesis. Otherwise, either:

- The proof t_1 has the form $inl(w_2)$ and the reduct is $(w_2/x)t_2$. As $inl(w_2) \in \llbracket A \vee B \rrbracket$, we have $w_2 \in \llbracket A \rrbracket$. Hence, $(w_2/x)t_2 \in \llbracket C \rrbracket$.

- The proof t_1 has the form $inr(w_3)$ and the reduct is $(w_3/x)t_3$. As $inr(w_3) \in \llbracket A \vee B \rrbracket$, we have $w_3 \in \llbracket B \rrbracket$. Hence, $(w_3/x)t_3 \in \llbracket C \rrbracket$.

- The proof t_1 has the form $t_1' \mathbin{+} t_1''$ and the reduct is $\delta_\vee(t_1', x.t_2, y.t_3) \mathbin{+} \delta_\vee(t_1'', x.t_2, y.t_3)$. As $t_1 \longrightarrow t_1'$ with an ultra-reduction rule, we have by Proposition 2.9, $t_1' \in \llbracket A \vee B \rrbracket$. In a similar way, $t_1'' \in \llbracket A \vee B \rrbracket$. Thus, by induction hypothesis, $\delta_\vee(t_1', x.t_2, y.t_3) \in \llbracket A \vee B \rrbracket$ and $\delta_\vee(t_1'', x.t_2, y.t_3) \in \llbracket A \vee B \rrbracket$. We conclude with Proposition 2.17.

- The proof t_1 has the form $\bullet t_1'$ and the reduct is $\bullet \delta_\vee(t_1', x.t_2, y.t_3)$. As $t_1 \longrightarrow t_1'$ with an ultra-reduction rule, we have by Proposition 2.9, $t_1' \in \llbracket A \vee B \rrbracket$. Thus, by induction hypothesis, $\delta_\vee(t_1', x.t_2, y.t_3) \in \llbracket A \vee B \rrbracket$. We conclude with Proposition 2.18. $\qquad\square$

Proposition 2.25 (Adequacy of $\delta_\odot$). *If $t_1 \in \llbracket A \odot B \rrbracket$, for all u in $\llbracket A \rrbracket$, $(u/x)t_2 \in \llbracket C \rrbracket$, and, for all v in $\llbracket B \rrbracket$, $(v/y)t_3 \in \llbracket C \rrbracket$, then $\delta_\odot(t_1, x.t_2, y.t_3) \in \llbracket C \rrbracket$.*

Proof. By Proposition 2.8, $x \in \llbracket A \rrbracket$, thus $t_2 = (x/x)t_2 \in \llbracket C \rrbracket$. In the same way, $t_3 \in \llbracket C \rrbracket$. Hence, t_1, t_2, and t_3 strongly terminate. We prove, by induction on $|t_1| + |t_2| + |t_3|$, that $\delta_\odot(t_1, x.t_2, y.t_3) \in \llbracket C \rrbracket$. Using Proposition 2.10, we only need to prove that every of its one step reducts is in $\llbracket C \rrbracket$. If the reduction takes place in t_1, t_2, or t_3, then we apply Proposition 2.9 and the induction hypothesis.

Otherwise, the proof t_1 has the form $[u, v]$ and the reduct is either $(u/x)t_2$ or $(v/x)t_3$. As $[u, v] \in \llbracket A \odot B \rrbracket$, we have $u \in \llbracket A \rrbracket$ and $v \in \llbracket B \rrbracket$. Hence, $(u/x)t_2 \in \llbracket C \rrbracket$ and $(v/x)t_3 \in \llbracket C \rrbracket$. $\qquad\square$

Proposition 2.26 (Adequacy of $\delta_\odot^1$). *If $t_1 \in \llbracket A \odot B \rrbracket$ and, for all u in $\llbracket A \rrbracket$, $(u/x)t_2 \in \llbracket C \rrbracket$, then $\delta_\odot^1(t_1, x.t_2) \in \llbracket C \rrbracket$.*

Proof. By Proposition 2.8, $x \in \llbracket A \rrbracket$, thus $t_2 = (x/x)t_2 \in \llbracket C \rrbracket$. Hence, t_1 and t_2 strongly terminate. We prove, by induction on $|t_1| + |t_2|$, that $\delta_\odot^1(t_1, x.t_2) \in \llbracket C \rrbracket$. Using Proposition 2.10, we only need to prove that every of its one step reducts is in $\llbracket C \rrbracket$. If the reduction takes place in t_1 or t_2, then we apply Proposition 2.9 and the induction hypothesis.

Otherwise, the proof t_1 has the form $[u, v]$ and the reduct is $(u/x)t_2$. As $[u, v] \in \llbracket A \odot B \rrbracket$, we have $u \in \llbracket A \rrbracket$. Hence, $(u/x)t_2 \in \llbracket C \rrbracket$. $\qquad\square$

Proposition 2.27 (Adequacy of $\delta_\odot^2$). *If $t_1 \in \llbracket A \odot B \rrbracket$ and, for all u in $\llbracket B \rrbracket$, $(u/x)t_2 \in \llbracket C \rrbracket$, then $\delta_\odot^2(t_1, x.t_2) \in \llbracket C \rrbracket$.*

Proof. By Proposition 2.8, $x \in \llbracket B \rrbracket$, thus $t_2 = (x/x)t_2 \in \llbracket C \rrbracket$. Hence, t_1 and t_2 strongly terminate. We prove, by induction on $|t_1| + |t_2|$, that $\delta_\odot^2(t_1, x.t_2) \in \llbracket C \rrbracket$. Using Proposition 2.10, we only need to prove that every of its one step reducts is in $\llbracket C \rrbracket$. If the reduction takes place in t_1 or t_2, then we apply Proposition 2.9 and the induction hypothesis.

Otherwise, the proof t_1 has the form $[u, v]$ and the reduct is $(v/x)t_2$. As $[u, v] \in \llbracket A \odot B \rrbracket$, we have $v \in \llbracket B \rrbracket$. Hence, $(v/x)t_2 \in \llbracket C \rrbracket$. $\qquad\square$

Theorem 2.28 (Adequacy). *Let t be a proof of A in a context $\Gamma = x_1 : A_1, ..., x_n : A_n$ and σ be a substitution mapping each variable x_i to an element of $\llbracket A_i \rrbracket$, then $\sigma t \in \llbracket A \rrbracket$.*

Proof. By induction on the structure of t.

If t is a variable, then, by definition of σ, $\sigma t \in \llbracket A \rrbracket$. For the seventeen other proof constructors, we use the Propositions 2.11 to 2.27. As all cases are similar, we just give a few examples.

- If $t = [u, v]$, where u is a proof of B and v a proof of C, then, by induction hypothesis, $\sigma u \in \llbracket B \rrbracket$ and $\sigma v \in \llbracket C \rrbracket$. Hence, by Proposition 2.16, $[\sigma u, \sigma v] \in \llbracket B \odot C \rrbracket$, that is $\sigma t \in \llbracket A \rrbracket$.

- If $t = \delta_\odot(u_1, x.u_2, y.u_3)$, where u_1 is a proof of $B \odot C$, u_2 a proof of A, and u_3 a proof of A, then, by induction hypothesis, $\sigma u_1 \in \llbracket B \odot C \rrbracket$, for all v in $\llbracket B \rrbracket$, $(v/x)\sigma u_2 \in \llbracket A \rrbracket$, and for all w in $\llbracket C \rrbracket$, $(w/x)\sigma u_3 \in \llbracket A \rrbracket$. Hence, by Proposition 2.25, $\delta_\odot(\sigma u_1, x.\sigma u_2, y.\sigma u_3) \in \llbracket A \rrbracket$, that is $\sigma t \in \llbracket A \rrbracket$. $\qquad\square$

Corollary 2.29 (Termination). *Let t be a proof of A in a context Γ. Then t strongly terminates.*

Proof. Let σ be the substitution mapping each variable $x_i : A_i$ of Γ to itself. Note that, by Proposition 2.8, this variable is an element of $\llbracket A_i \rrbracket$. Then $t = \sigma t$ is an element of $\llbracket A \rrbracket$. Hence, it strongly terminates. $\qquad\square$

2.6. Introduction property

Theorem 2.30 (Introduction)**.** *Let t be a closed irreducible proof of A.*

- *If A has the form $\top$, then t is $\star$.*

- *The proposition A is not $\bot$.*

- *If A has the form $B \Rightarrow C$, then t has the form $\lambda x.u$.*

- *If A has the form $B \wedge C$, then t has the form $\langle u, v \rangle$.*

- *If A has the form $B \vee C$, then t has the form $inl(u)$, $inr(u)$, $u + v$, or $\bullet u$.*

- *If A has the form $B \odot C$, then t has the form $[u, v]$.*

Proof. By induction on the structure of t.

We first remark that, as the proof t is closed, it is not a variable. Then, we prove that it cannot be an elimination.

- If $t = \delta_\top(u, v)$, then u is a closed irreducible proof of $\top$, hence, by induction hypothesis, it is $\star$ and the proof t is reducible.

- If $t = \delta_\bot(u)$, then u is a closed irreducible proof of $\bot$ and, by induction hypothesis, no such proofs exist.

- If $t = u\ v$, then u is a closed irreducible proof of $B \Rightarrow A$, hence, by induction hypothesis, it has the form $\lambda x.u_1$ and the proof t is reducible.

- If $t = \delta_\wedge^1(u, x.v)$, then u is a closed irreducible proof of $B \wedge C$, hence, by induction hypothesis, it has the form $\langle u_1, u_2 \rangle$ and the proof t is reducible.

- If $t = \delta_\wedge^2(u, x.v)$, then u is a closed irreducible proof of $B \wedge C$, hence, by induction hypothesis, it has the form $\langle u_1, u_2 \rangle$ and the proof t is reducible.

- If $t = \delta_\vee(u, x.v, y.w)$, then u is a closed irreducible proof of $B \vee C$, hence, by induction hypothesis, it has the form $inl(u_1)$, $inr(u_1)$, $u_1 + u_2$, or $\bullet u_1$ and the proof t is reducible.

- If $t = \delta_\odot(u, x.v, y.w)$, $t = \delta_\odot^1(u, x.v)$, or $t = \delta_\odot^2(u, x.v)$, then u is a closed irreducible proof of $B \odot C$, hence, by induction hypothesis, it has the form $[u_1, u_2]$ and the proof t is reducible.

Hence, t is an introduction, a sum, or a product.

It t is $\star$, then A is $\top$. If it has the form $\lambda x.u$, then A has the form $B \Rightarrow C$. If it has the form $\langle u, v \rangle$, then A has the form $B \wedge C$. If it has the form $inl(u)$ or $inr(u)$, then A has the form $B \vee C$. If it has the form $[u, v]$ then A has the form $B \odot C$. We prove that, if it has the form $u + v$ or $\bullet u$, A has the form $B \vee C$.

- If $t = u + v$, then the proofs u and v are two closed and irreducible proofs of A. If $A = \top$ then, by induction hypothesis, they are both $\star$ and the proof t is reducible. If $A = \bot$ then, they are irreducible proofs of $\bot$ and, by induction hypothesis, no such proofs exist. If A has the form $B \Rightarrow C$ then, by induction hypothesis, they are both abstractions and the proof t is reducible. If A has the form $B \wedge C$, then, by induction hypothesis, they are both pairs and the proof t is reducible. If A has the form $B \odot C$, then, by induction hypothesis, they are both superpositions and the proof t is reducible. Hence, A has the form $B \vee C$.

- If $t = \bullet u$, then the proofs u is a closed and irreducible proof of A. If $A = \top$ then, by induction hypothesis, u is $\star$ and the proof t is reducible. If $A = \bot$ then, it is an irreducible proof of $\bot$ and, by induction hypothesis, no such proofs exist. If A has the form $B \Rightarrow C$ then, by induction hypothesis, it is an abstraction and the proof t is reducible. If A has the form $B \wedge C$, then, by induction hypothesis, it is a pair and the proof t is reducible. If A has the form $B \odot C$, then, by induction hypothesis, it is a superposition and the proof t is reducible. Hence, A has the form $B \vee C$. □

16

Note that we reap here the benefit of commuting, when possible, the interstitial rules with the introduction rules, as, except for the disjunction, closed irreducible proofs are genuine introductions.

Proposition 2.31 (Disjunction). *If the proposition $A \vee B$ has a closed proof, then A has a closed proof or B has a closed proof.*

Proof. Consider a closed proof of $A \vee B$ and its irreducible form t. We prove, by induction on the structure of t, that A has a closed proof or B has a closed proof. By Theorem 2.30, t has the form $inl(u)$, $inr(u)$, $u \mathbin{+} v$, or $\bullet u$. If it has the form $inl(u)$, u is a closed proof of A. If it has the form $inr(u)$, u is a closed proof of B. If it has the form $u \mathbin{+} v$ or $\bullet u$, u is a closed irreducible proof of $A \vee B$. Thus, by induction hypothesis, A has a closed proof or B has a closed proof. $\square$

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.

One way to do so is to consider a field $\mathcal{S}$ of *scalars*, for instance $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, take a different rule $\top$-i for each scalar and a different rule prod for each scalar. So, for each scalar a, we have a closed irreducible proof of $\top$ and we write $a.\star$ for this proof. In the same way, we write $a \bullet t$ for the proof obtained by applying, to the proof t, the rule prod corresponding to the scalar a. As the closed irreducible proofs of $\top$ are in one-to-one correspondence with the elements of $\mathcal{S}$, those of $\top \odot \top$ are in one-to-one with the elements of $\mathcal{S}^2$, those of $(\top \odot \top) \odot (\top \odot \top)$ are in one-to-one correspondence with the elements of $\mathcal{S}^4$, etc.

In the $\odot$-calculus, the proof $\star \mathbin{+} \star$ reduces to $\star$. Now, the proof $a.\star \mathbin{+} b.\star$ reduces to $(a + b).\star$, where the scalars are added. In the same way the proof $a \bullet b.\star$ reduces to $(a \times b).\star$, where the scalars are multiplied. In the $\odot$-calculus, the proof $\delta_\top(\star, t)$ reduces to $\bullet t$. Now, the proof $\delta_\top(a.\star, t)$ does not reduce to $\bullet t$, or to t, but to $a \bullet t$.

3.1. The $\odot^{\mathcal{S}}$-calculus

We define the $\odot^{\mathcal{S}}$-calculus (read: "the sup-S-calculus"), by extending the grammar of proofs as follows

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

where a is a scalar.

The typing rules are similar to those of Figure 2 except the rule

$$\frac{}{\Gamma \vdash \star : \top}\ \top\text{-i}$$

which is replaced with

$$\frac{}{\Gamma \vdash a.\star : \top}\ \top\text{-i}(a)$$

and the rule

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \bullet t : A}\ \text{prod}$$

which is replaced with

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash a \bullet t : A}\ \text{prod}(a)$$

The reduction rules are those of Figure 4.

The $\odot^{\mathcal{S}}$-calculus is thus a λ-calculus equipped with a notion of linear combination of terms, such as Lineal [2], the Algebraic λ-calculus [24], etc.

17

$$\delta_\top(a.\star, t) \longrightarrow a \bullet t$$
$$(\lambda x.t)\ u \longrightarrow (u/x)t$$
$$\delta_\wedge^1(\langle t, u \rangle, x.v) \longrightarrow (t/x)v$$
$$\delta_\wedge^2(\langle t, u \rangle, x.v) \longrightarrow (u/x)v$$
$$\delta_\vee(inl(t), x.v, y.w) \longrightarrow (t/x)v$$
$$\delta_\vee(inr(u), x.v, y.w) \longrightarrow (u/y)w$$
$$\delta_\odot([t, u], x.v, y.w) \longrightarrow (t/x)v$$
$$\delta_\odot([t, u], x.v, y.w) \longrightarrow (u/y)w$$
$$\delta_\odot^1([t, u], x.v) \longrightarrow (t/x)v$$
$$\delta_\odot^2([t, u], x.v) \longrightarrow (u/x)v$$

$$a.\star \mathbin{\boldsymbol{+}} b.\star \longrightarrow (a + b).\star$$
$$(\lambda x.t) \mathbin{\boldsymbol{+}} (\lambda x.u) \longrightarrow \lambda x.(t \mathbin{\boldsymbol{+}} u)$$
$$\langle t, u \rangle \mathbin{\boldsymbol{+}} \langle v, w \rangle \longrightarrow \langle t \mathbin{\boldsymbol{+}} v, u \mathbin{\boldsymbol{+}} w \rangle$$
$$\delta_\vee(t \mathbin{\boldsymbol{+}} u, x.v, y.w) \longrightarrow \delta_\vee(t, x.v, y.w) \mathbin{\boldsymbol{+}} \delta_\vee(u, x.v, y.w)$$
$$[t, u] \mathbin{\boldsymbol{+}} [v, w] \longrightarrow [t \mathbin{\boldsymbol{+}} v, u \mathbin{\boldsymbol{+}} w]$$

$$a \bullet b.\star \longrightarrow (a \times b).\star$$
$$a \bullet \lambda x.t \longrightarrow \lambda x.a \bullet t$$
$$a \bullet \langle t, u \rangle \longrightarrow \langle a \bullet t, a \bullet u \rangle$$
$$\delta_\vee(a \bullet t, x.v, y.w) \longrightarrow a \bullet \delta_\vee(t, x.v, y.w)$$
$$a \bullet [t, u] \longrightarrow [a \bullet t, a \bullet u]$$

Figure 4: The reduction rules of the $\odot^{\mathcal{S}}$-calculus

3.2. Properties

Theorem 3.1 (Subject reduction). *If $\Gamma \vdash t : A$ and $t \longrightarrow u$, then $\Gamma \vdash u : A$.*

Proof. We first prove a substitution lemma and then proceed by induction on the definition of the relation $\longrightarrow$. $\qquad\square$

Theorem 3.2 (Confluence). *This system of Figure 4 without the rules*

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

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

is confluent.

Proof. This system also is left linear and it has no critical pairs. Thus, by [12, Theorem 6.8] it is confluent. $\qquad\square$

Theorem 3.3 (Termination). *Let t be a proof of A in a context Γ. Then t strongly terminates.*

Proof. Consider a translation $^\circ$ of proofs from the $\odot^{\mathcal{S}}$-calculus to the $\odot$-calculus obtained by replacing the rules $\top$-i(a) with the rule $\top$-i and the rules prod(a) with the rule prod: $(a.\star)^\circ = \star$, $(a \bullet t)^\circ = \bullet t^\circ$, etc. If $t \longrightarrow u$ in the $\odot^{\mathcal{S}}$-calculus, then $t^\circ \longrightarrow u^\circ$ in the $\odot$-calculus. Hence, the reduction in the $\odot^{\mathcal{S}}$-calculus terminates. $\qquad\square$

Theorem 3.4 (Introduction). *Let t be a closed irreducible proof of A.*

- *If A has the form $\top$, then t is $a.\star$.*

- *The proposition A is not $\bot$.*

18

- *If A has the form $B \Rightarrow C$, then t has the form $\lambda x.u$.*

- *If A has the form $B \wedge C$, then t has the form $\langle u, v \rangle$.*

- *If A has the form $B \vee C$, then t has the form $inl(u)$, $inr(u)$, $u \mathbin{\text{\textbf{+}}} v$, or $a \bullet u$.*

- *If A has the form $B \odot C$, then t has the form $[u, v]$.*

Proof. Similar to that of Theorem 2.30. $\qquad\square$

3.3. Quantifying non-determinism

When $\mathcal{S}$ is $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, we can use the scalars a and b to assign probabilities to the reductions

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

and

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

Example 3.5. *We define a strategy where the rules*

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

and

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

apply only when t and u are closed irreducible proofs.

In this case, if a and b are not both 0, we assign the probabilities $\frac{|a|^2}{|a|^2+|b|^2}$ and $\frac{|b|^2}{|a|^2+|b|^2}$ to the reductions

$$\delta_\odot([a.\star, b.\star], x.v, y.w) \longrightarrow (a.\star/x)v$$

and

$$\delta_\odot([a.\star, b.\star], x.v, y.w) \longrightarrow (b.\star/y)w$$

And if either $a = b = 0$ or t and u are proofs of propositions different from $\top$, we assign any probability, for instance $\frac{1}{2}$, to these reductions.

4. Application to quantum computing

We now show that the $\odot^{\mathbb{C}}$-calculus, with the reduction strategy of Example 3.5, restricting the reduction of $\delta_\odot([t, u], x.v, y.w)$ to the cases where t and u are closed irreducible proofs, contains the core of a small quantum programming language.

4.1. Bits

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

Note that the proofs $inl(1.\star)$ and $inr(1.\star)$ are not the only closed irreducible proofs of $\mathcal{B}$, for example $inl(2.\star)$ and $inl(1.\star) \mathbin{\text{\textbf{+}}} inr(1.\star)$ also are.

Definition 4.2 (Test). *The test operator is defined as*

$$If(t, u, v) = \delta_\vee(t, x.u, y.v)$$

where x and y are variables not occurring in u and v. Note that $If(\mathbf{0}, u, v) \longrightarrow u$ and $If(\mathbf{1}, u, v) \longrightarrow v$.

A n-qubit, for $n \geq 1$, is a vector of $\mathbb{C}^{2^n}$ of norm 1. We show now how n-qubits, and more generally vectors of $\mathbb{C}^{2^n}$, for $n \geq 0$, can be expressed as proofs in the $\odot^{\mathbb{C}}$-calculus.

Definition 4.3 (The proposition $\mathcal{Q}^{\otimes n}$). *The proposition $\mathcal{Q}^{\otimes n}$ is defined by induction on n as follows*

- $\mathcal{Q}^{\otimes 0} = \top$,

- $\mathcal{Q}^{\otimes n+1} = \mathcal{Q}^{\otimes n} \odot \mathcal{Q}^{\otimes n}$.

Note that, in this definition, the binary connective $\odot$ is always used with two identical propositions: $A \odot A$.

The proposition $\mathcal{Q}^{\otimes 1} = \top \odot \top$ is sometimes written $\mathcal{Q}$.

The closed irreducible proofs of $\mathcal{Q}^{\otimes n}$ and the vectors of $\mathbb{C}^{2^n}$ are in one-to-one correspondence: to each closed irreducible proof t of $\mathcal{Q}^{\otimes n}$, we associate a vector $\underline{t}$ of $\mathbb{C}^{2^n}$ and to each vector $\mathbf{u}$ of $\mathbb{C}^{2^n}$, we associate a closed irreducible proof $\overline{\mathbf{u}}$ of $\mathcal{Q}^{\otimes n}$.

Definition 4.4 (One-to-one correspondance). *To each closed irreducible proof t of $\mathcal{Q}^{\otimes n}$, we associate a vector $\underline{t}$ of $\mathbb{C}^{2^n}$ as follows.*

- *If $n = 0$, then $t = a.\star$. We let $\underline{t} = (\,a\,)$.*

- *If $n = n' + 1$, then $t = [u, v]$. We let $\underline{t}$ be the vector with two blocks $\underline{u}$ and $\underline{v}$: $\underline{t} = (\frac{\underline{u}}{\underline{v}})$.*

To each vector $\mathbf{u}$ of $\mathbb{C}^{2^n}$, we associate a closed irreducible proof $\overline{\mathbf{u}}$ of $\mathcal{Q}^{\otimes n}$.

- *If $n = 0$, then $\mathbf{u} = (\,a\,)$. We let $\overline{\mathbf{u}} = a.\star$.*

- *If $n = n' + 1$, let $\mathbf{u}_1$ and $\mathbf{u}_2$ be the two blocks of $\mathbf{u}$ of $2^{n'}$ lines, so $\mathbf{u} = (\frac{\mathbf{u}_1}{\mathbf{u}_2})$. We let $\overline{\mathbf{u}} = [\overline{\mathbf{u}_1}, \overline{\mathbf{u}_2}]$.*

In particular, the proof $0_{\mathcal{Q}^{\otimes n}}$ is defined as $\overline{\mathbf{0}}$, where $\mathbf{0}$ is the zero vector of $\mathbb{C}^{2^n}$.

Example 4.5. *The 2-qubit $|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ is expressed as the proof $\overline{|01\rangle} = [[0.\star, 1.\star], [0.\star, 0.\star]]$ and the entangled 2-qubit $\frac{1}{\sqrt{2}}.|00\rangle + \frac{1}{\sqrt{2}}.|11\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ as the proof $\overline{\frac{1}{\sqrt{2}}.|00\rangle + \frac{1}{\sqrt{2}}.|11\rangle} = [[\frac{1}{\sqrt{2}}.\star, 0.\star], [0.\star, \frac{1}{\sqrt{2}}.\star]]$.*

We extend the definition of $\underline{t}$ to any closed proof of $\mathcal{Q}^{\otimes n}$, $\underline{t}$ is by definition $\underline{t'}$, where t' is the irreducible form of t.

We also take the convention that any closed irreducible proof u of $\mathcal{Q}^{\otimes n}$, expressing a non-zero vector $\underline{u} \in \mathbb{C}^{2^n}$, is an alternative expression of the n-qubit $\frac{\underline{u}}{\|\underline{u}\|}$. For example, the qubit $\frac{1}{\sqrt{2}}.|0\rangle + \frac{1}{\sqrt{2}}.|1\rangle$ is expressed as the proof $[\frac{1}{\sqrt{2}}.\star, \frac{1}{\sqrt{2}}.\star]$, but also as the proof $[1.\star, 1.\star] = \overline{|0\rangle + |1\rangle}$.

The next lemmas show that the symbol $\boldsymbol{+}$ expresses the sum of vectors and the symbol $\bullet$, the product of a vector by a scalar.

Proposition 4.6 (Sum of vectors). *Let u and v be two closed proofs of $\mathcal{Q}^{\otimes n}$. Then, $\underline{u \boldsymbol{+} v} = \underline{u} + \underline{v}$.*

Proof. By induction on n.

- If $n = 0$, then $u \longrightarrow^* a.\star$, $v \longrightarrow^* b.\star$, $\underline{u} = (\,a\,)$, $\underline{v} = (\,b\,)$. Thus, $\underline{u \boldsymbol{+} v} = \underline{a.\star \boldsymbol{+} b.\star} = \underline{(a + b).\star} = (\,a+b\,) = (\,a\,) + (\,b\,) = \underline{u} + \underline{v}$.

- If $n = n' + 1$, then $u \longrightarrow^* [u_1, u_2]$, $v \longrightarrow^* [v_1, v_2]$, $\underline{u} = (\frac{u_1}{u_2})$ and $\underline{v} = (\frac{v_1}{v_2})$. Thus, using the induction hypothesis, $\underline{u \boldsymbol{+} v} = \underline{[u_1, u_2] \boldsymbol{+} [v_1, v_2]} = \underline{[u_1 \boldsymbol{+} v_1, u_2 \boldsymbol{+} v_2]} = \left(\frac{\underline{u_1 \boldsymbol{+} v_1}}{\underline{u_2 \boldsymbol{+} v_2}}\right) = \left(\frac{\underline{u_1} + \underline{v_1}}{\underline{u_2} + \underline{v_2}}\right) = (\frac{\underline{u_1}}{\underline{u_2}}) + (\frac{\underline{v_1}}{\underline{v_2}}) = \underline{u} + \underline{v}$. $\square$

Proposition 4.7 (Product of a vector by a scalar). *Let u be a closed proof of $\mathcal{Q}^{\otimes n}$. Then $\underline{a \bullet u} = a\underline{u}$.*

Proof. By induction on n.

- If $n = 0$, then $u \longrightarrow^* b.\star$, $\underline{u} = (\,b\,)$. Thus, $\underline{a \bullet u} = \underline{a \bullet b.\star} = \underline{(a \times b).\star} = (\,a \times b\,) = a\,(\,b\,) = a\underline{u}$.

- If $n = n' + 1$, $u \longrightarrow^* \langle u_1, u_2 \rangle$, $\underline{u} = \left(\begin{smallmatrix}u_1\\u_2\end{smallmatrix}\right)$. Thus, using the induction hypothesis, $\underline{a \bullet u} = \underline{a \bullet \langle u_1, u_2 \rangle} = \underline{\langle a \bullet u_1, a \bullet u_2 \rangle} = \left(\begin{smallmatrix}\underline{a \bullet u_1}\\\underline{a \bullet u_2}\end{smallmatrix}\right) = \left(\begin{smallmatrix}a\underline{u_1}\\a\underline{u_2}\end{smallmatrix}\right) = a\left(\begin{smallmatrix}\underline{u_1}\\\underline{u_2}\end{smallmatrix}\right) = a\underline{u}$. $\qquad\square$

4.3. Matrices

The information-preserving, reversible, and deterministic unitary operators are expressed with the proof constructors $\delta^1_\odot$ and $\delta^2_\odot$.

Theorem 4.8 (Matrices). *Let M be a matrix with 2^m columns and 2^n lines, then there exists a closed proof t of $\mathcal{Q}^{\otimes m} \Rightarrow \mathcal{Q}^{\otimes n}$ such that, for all vectors $\mathbf{u} \in \mathbb{C}^{2^m}$, $t\,\underline{\mathbf{u}} = M\mathbf{u}$.*

Proof. By induction on A.

- If $m = 0$, then M is a matrix of one column and 2^n lines. Hence, it is also a vector of 2^n lines. We take
$$t = \lambda x.\delta_\top(x, \overline{M})$$
Let $\mathbf{u} \in \mathcal{S}^1$, $\mathbf{u}$ has the form $(\,a\,)$ and $\overline{\mathbf{u}} = a.\star$. Hence, using Proposition 4.7, we have $\underline{t\,\overline{\mathbf{u}}} = \underline{\delta_\top(\overline{\mathbf{u}}, \overline{M})} = \underline{\delta_\top(a.\star, \overline{M})} = \underline{a \bullet \overline{M}} = a\underline{\overline{M}} = aM = M(\,a\,) = M\mathbf{u}$.

- If $m = m' + 1$, then let M_1 and M_2 be the two blocks of M of $2^{m'}$ columns, so $M = (\,M_1 \ M_2\,)$.

  By induction hypothesis, there exist closed proofs t_1 and t_2 of the proposition $\mathcal{Q}^{m'} \Rightarrow \mathcal{Q}^n$ such that, for all vectors $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{C}^{2^{m'}}$, we have $\underline{t_1\,\overline{\mathbf{u}_1}} = M_1\mathbf{u}_1$ and $\underline{t_2\,\overline{\mathbf{u}_2}} = M_2\mathbf{u}_2$. We take
$$t = \lambda x.(\delta^1_\odot(x, y.(t_1\ y)) \mathbf{+} \delta^2_\odot(x, z.(t_2\ z)))$$
Let $\mathbf{u} \in \mathbb{C}^{2^m}$, and $\mathbf{u}_1$ and $\mathbf{u}_2$ be the two blocks of $2^{m'}$ lines of $\mathbf{u}$, so $\mathbf{u} = \left(\begin{smallmatrix}\mathbf{u}_1\\\mathbf{u}_2\end{smallmatrix}\right)$, and $\overline{\mathbf{u}} = [\overline{\mathbf{u}_1}, \overline{\mathbf{u}_2}]$.

  Then, using Proposition 4.6, $\underline{t\,\overline{\mathbf{u}}} = \underline{\delta^1_\odot([\overline{\mathbf{u}_1}, \overline{\mathbf{u}_2}], y.(t_1\ y)) \mathbf{+} \delta^2_\odot([\overline{\mathbf{u}_1}, \overline{\mathbf{u}_2}], z.(t_2\ z))} = \underline{t_1\,\overline{\mathbf{u}_1} \mathbf{+} t_2\,\overline{\mathbf{u}_2}} = \underline{t_1\,\overline{\mathbf{u}_1}} + \underline{t_2\,\overline{\mathbf{u}_2}} = M_1\mathbf{u}_1 + M_2\mathbf{u}_2 = (\,M_1\ M_2\,)\left(\begin{smallmatrix}\mathbf{u}_1\\\mathbf{u}_2\end{smallmatrix}\right) = M\mathbf{u}$. $\qquad\square$

Example 4.9 (Matrices with two colums and two lines). *The matrix $\left(\begin{smallmatrix}a & c\\b & d\end{smallmatrix}\right)$ is expressed as the proof*
$$t = \lambda x.(\delta^1_\odot(x, y.\delta_\top(y, [a.\star, b.\star])) \mathbf{+} \delta^2_\odot(x, z.\delta_\top(z, [c.\star, d.\star])))$$
Then
$$\begin{aligned}
t\ [e.\star, f.\star] &\longrightarrow \delta^1_\odot([e.\star, f.\star], y.\delta_\top(y, [a.\star, b.\star])) \mathbf{+} \delta^2_\odot([e.\star, f.\star], z.\delta_\top(z, [c.\star, d.\star]))\\
&\longrightarrow^* \delta_\top(e.\star, [a.\star, b.\star]) \mathbf{+} \delta_\top(f.\star, [c.\star, d.\star])\\
&\longrightarrow^* e \bullet [a.\star, b.\star] \mathbf{+} f \bullet [c.\star, d.\star]\\
&\longrightarrow^* [(a \times e).\star, (b \times e).\star] \mathbf{+} [(c \times f).\star, (d \times f).\star]\\
&\longrightarrow^* [(a \times e + c \times f).\star, (b \times e + d \times f).\star]
\end{aligned}$$

For instance, the Hadamard matrix $H = \left(\begin{smallmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}}\end{smallmatrix}\right)$ is expressed as the proof
$$\lambda x.\delta^1_\odot(x, y.\delta_\top(y, [\tfrac{1}{\sqrt{2}}.\star, \tfrac{1}{\sqrt{2}}.\star])) \mathbf{+} \delta^2_\odot(x, z.\delta_\top(z, [\tfrac{1}{\sqrt{2}}.\star, \tfrac{-1}{\sqrt{2}}.\star]))$$

$$\pi_n = \lambda x.\delta_\odot(x, y.[y, 0_{\mathcal{Q}^{\otimes n-1}}], z.[0_{\mathcal{Q}^{\otimes n-1}}, z])$$
$$\pi'_n = \lambda x.\delta_\odot(x, y.\mathbf{0}, z.\mathbf{1})$$
$$\pi''_n = \lambda x.\delta_\odot(x, y.\langle[y, 0_{\mathcal{Q}^{\otimes n-1}}], \mathbf{0}\rangle, z.\langle[0_{\mathcal{Q}^{\otimes n-1}}, z], \mathbf{1}\rangle)$$

Figure 5: Measurement operators

4.4. Probabilities

Definition 4.10 (Norm). *Let t be a closed irreducible proof of $\mathcal{Q}^{\otimes n}$, we define the square of the norm $\|t\|^2$ of t by induction on n.*

- *If $n = 0$, then $t = a.\star$ and we take $\|t\|^2 = |a|^2$.*

- *If $n = n' + 1$, then $t = [u_1, u_2]$ and we take $\|t\|^2 = \|u_1\|^2 + \|u_2\|^2$.*

If t is a closed irreducible proof of $\mathcal{Q}^{\otimes n}$ of the form $[u_1, u_2]$, where $\|u_1\|^2$ and $\|u_2\|^2$ are not both 0, then we assign the probability $\frac{\|u_1\|^2}{\|u_1\|^2 + \|u_2\|^2}$ to the reduction

$$\delta_\odot([u_1, u_2], x.v, y.w) \longrightarrow (u_1/x)v$$

and the probability $\frac{\|u_2\|^2}{\|u_1\|^2 + \|u_2\|^2}$ to the reduction

$$\delta_\odot([u_1, u_2], x.v, y.w) \longrightarrow (u_2/y)w$$

If $\|u_1\|^2 = \|u_2\|^2 = 0$, or u_1 and u_2 are proofs of propositions of a different form, we associate any probability, for example $\frac{1}{2}$, to both reductions.

Example 4.11. *If t is a closed irreducible proof of $\mathcal{Q}$ of the form $[a.\star, b.\star]$, where a and b are not both 0, then we assign the probability $\frac{|a|^2}{|a|^2 + |b|^2}$ to the reduction*

$$\delta_\odot([a.\star, b.\star], x.v, y.w) \longrightarrow (a.\star/x)v$$

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

$$\delta_\odot([a.\star, b.\star], x.v, y.w) \longrightarrow (b.\star/y)w$$

If t is a closed irreducible proof of $\mathcal{Q}^{\otimes 2}$ of the form $[[a.\star, b.\star], [c.\star, d.\star]]$ 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

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

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

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

4.5. Measure

The information-erasing, non-reversible, and non-deterministic measurement operators are expressed with the proof constructor $\delta_\odot$.

Several such operators are defined in Figure 5. Let n be a non-zero natural number and t be a closed irreducible proof of $\mathcal{Q}^{\otimes n}$ of the form $[u_1, u_2]$, such that $\|t\|^2 = \|u_1\|^2 + \|u_2\|^2 \neq 0$, expressing the state of an n-qubit. The proof $\pi_n\, t$ of the proposition $\mathcal{Q}^{\otimes n}$ reduces, with probabilities $\frac{\|u_1\|^2}{\|u_1\|^2 + \|u_2\|^2}$ and $\frac{\|u_2\|^2}{\|u_1\|^2 + \|u_2\|^2}$ to $[u_1, 0_{\mathcal{Q}^{\otimes n-1}}]$ and to $[0_{\mathcal{Q}^{\otimes n-1}}, u_2]$. It is the state of the n-qubit, after the partial measure of the first qubit. The proof $\pi'_n\, t$ of the proposition $\mathcal{B}$ reduces, with the same probabilities, to $\mathbf{0}$ and to $\mathbf{1}$. It is the "classical" result of the measure. The proof $\pi''_n\, t$ of the proposition $\mathcal{Q}^{\otimes n} \wedge \mathcal{B}$ reduces, with the same probabilities, to $\langle[u_1, 0_{\mathcal{Q}^{\otimes n-1}}], \mathbf{0}\rangle$ and to $\langle[0_{\mathcal{Q}^{\otimes n-1}}, u_2], \mathbf{1}\rangle$. It is the pair formed with the state of the n-qubit, after the measure, and the "classical" result of the measure.

22

Example 4.12. *In the case* $n = 1$*, if* t *is a closed irreducible proof of* $\mathcal{Q}^{\otimes 1}$ *of the form* $[a.\star, b.\star]$*, such that* a *and* b *are not both* 0*, then the proof* $\pi_1\ t$ *of the proposition* $\mathcal{Q}^{\otimes 1}$ *reduces, with probabilities* $\frac{|a|^2}{|a|^2+|b|^2}$ *and* $\frac{|b|^2}{|a|^2+|b|^2}$*, to* $[a.\star, 0.\star]$*, that is an expression of* $|0\rangle$*, and to* $[0.\star, b.\star]$*, that is an expression of* $|1\rangle$*. The proof* $\pi_1'\ t$ *of the proposition* $\mathcal{B}$ *reduces, with the same probabilities, to* $\mathbf{0}$ *and to* $\mathbf{1}$*. The proof* $\pi_1''\ t$ *of the proposition* $\mathcal{Q}^{\otimes 1} \wedge \mathcal{B}$ *reduces, with the same probabilities, to* $\langle[a.\star, 0.\star], \mathbf{0}\rangle$ *and to* $\langle[0.\star, b.\star], \mathbf{1}\rangle$*.*

Example 4.13. *In the case* $n = 2$*, if* t *is a closed irreducible proof of* $\mathcal{Q}^{\otimes 2}$ *of the form* $[[a.\star, b.\star], [c.\star, d.\star]]$ *where* a*,* b*,* c*, and* d *are not all* 0*, then the proof* $\pi_2\ t$ *of the proposition* $\mathcal{Q}^{\otimes 2}$ *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* $[[a.\star, b.\star], [0.\star, 0.\star]]$ *and to* $[[0.\star, 0.\star], [c.\star, d.\star]]$*. The proof* $\pi_2'\ t$ *of the proposition* $\mathcal{B}$ *reduces, with the same probabilities, to* $\mathbf{0}$ *and to* $\mathbf{1}$*. The proof* $\pi_2''\ t$ *of the proposition* $\mathcal{Q}^{\otimes 2} \wedge \mathcal{B}$ *reduces, with the same probabilities, to* $\langle[[a.\star, b.\star], [0.\star, 0.\star]], \mathbf{0}\rangle$ *and to* $\langle[[0.\star, 0.\star], [c.\star, d.\star]], \mathbf{1}\rangle$*.*

Using the representation of matrices, it is possible to define measurement operators that measure in any basis, by changing basis, measuring, and changing basis again. This way, it is also possible to define measurement operators that partially measure, not the first qubit of a n-qubit, but any.

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

$$
U_f = \begin{pmatrix}
if(f0,1,0) & if(f0,0,1) & 0 & 0 \\
if(f0,0,1) & if(f0,1,0) & 0 & 0 \\
0 & 0 & if(f1,1,0) & if(f1,0,1) \\
0 & 0 & if(f1,0,1) & if(f1,1,0)
\end{pmatrix}
$$

   where $if(0, n, m) = n$ and $if(1, n, m) = m$.
   Note that $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$ for $x, y \in \{0, 1\}$, where $\oplus$ is the exclusive disjunction.
3. Apply to it the unitary operator

$$
H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}
$$

4. Measure the first qubit. The output is 0, if f is constant and 1 if it is not.

In the $\odot^{\mathbb{C}}$-calculus, the initial state is

$$
\overline{|+-\rangle} = [[\frac{1}{2}.\star, \frac{-1}{2}.\star], [\frac{1}{2}.\star, \frac{-1}{2}.\star]]
$$

the function mapping the function f to the operator U_f is expressed as in the proof of Theorem 4.8

$$
U = \lambda f.\lambda t.(\delta_{\odot}^1(t, x.(\delta_{\odot}^1(x, z_0.M_0\ z_0) \mathbin{\text{\textbf{+}}} \delta_{\odot}^2(x, z_1.M_1\ z_1))) \mathbin{\text{\textbf{+}}} \delta_{\odot}^2(t, y.(\delta_{\odot}^1(y, z_2.\ M_2\ z_2) \mathbin{\text{\textbf{+}}} \delta_{\odot}^2(y, z_3.\ M_3\ z_3))))
$$

with

$$
M_0 = \lambda s.\delta_\top(s, If(f\ \mathbf{0}, [[1.\star, 0.\star], [0.\star, 0.\star]], [[0.\star, 1.\star], [0.\star, 0.\star]]))
$$

$$
M_1 = \lambda s.\delta_\top(s, If(f\ \mathbf{0}, [[0.\star, 1.\star], [0.\star, 0.\star]], [[1.\star, 0.\star], [0.\star, 0.\star]]))
$$

$$
M_2 = \lambda s.\delta_\top(s, If(f\ \mathbf{1}, [[0.\star, 0.\star], [1.\star, 0.\star]], [[0.\star, 0.\star], [0.\star, 1.\star]]))
$$

$$
M_3 = \lambda s.\delta_\top(s, If(f\ \mathbf{1}, [[0.\star, 0.\star], [0.\star, 1.\star]], [[0.\star, 0.\star], [1.\star, 0.\star]]))
$$

The operator $H \otimes I$ is also expressed as in the proof of Theorem 4.8 and Deutsch's algorithm is the proof of $(\mathcal{B} \Rightarrow \mathcal{B}) \Rightarrow \mathcal{B}$

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

Let f be a proof of $\mathcal{B} \Rightarrow \mathcal{B}$. If f is a constant function, we have $Deutsch\ f \longrightarrow^* \mathbf{0}$, while if f if not constant, $Deutsch\ f \longrightarrow^* \mathbf{1}$.

5. Conclusion

We have extended the propositional logic with a connective $\odot$, that has both excessive and harmonious deduction rules, and with interstitial rules. We have then extended this logic again with scalars. We have shown that the proof language of this logic forms the core of a quantum programming language.

The connective $\odot$, with its elimination symbol $\delta_\odot$, models information-erasure, non-reversibility, and non-determinism, that occur, for example, in quantum measurement. With its elimination symbols $\delta_\odot^1$ and $\delta_\odot^2$, it models the information-preservation, reversibility, and determinism that occur, for example, in unitary transformations.

There are several points that we did not address in this paper. First, we leave open the question of the interpretation of this logic in a model, in particular a categorical one, besides the obvious Lindenbaum algebra.

Then, these notions of insufficient and excessive deduction rules are not specific to natural deduction and similar notions could be defined and investigated, for instance, in sequent calculus. Note that in the sequent calculus, harmony can be defined in a stronger sense, that includes, not only the possibility to reduce proofs, but also to reduce the use of the rule axiom on non-atomic propositions to smaller ones [13]—an analog of the η-expansion, but generalized to arbitrary connectives.

Finally, the $\odot^{\mathbb{C}}$-calculus can express all quantum circuits, as it can express matrices and measurement operators. However, it is not restricted to quantum algorithms, since the $\odot$ connective addresses the question of the information-erasure, non-reversibility, and non-determinism of measurement, but not that of linearity and unitarity. We leave for future work the restriction of the calculus to linear operators, forbidding, for example, the non-linear proof of the proposition $\mathcal{Q} \Rightarrow \mathcal{Q}^{\otimes 2}$

$$\lambda x.\delta_\odot^1(x, y.\delta_\odot^1(x, y_1.[[\delta_\top(y, y_1), 0.\star], [0.\star, 0.\star]]) + \delta_\odot^2(x, z_1.[[0.\star, \delta_\top(y, z_1)], [0.\star, 0.\star]]))$$
$$+$$
$$\delta_\odot^2(x, z.\delta_\odot^1(x, y_2.[[0.\star, 0.\star], [\delta_\top(z, y_2), 0.\star]]) + \delta_\odot^2(x, z_2.[[0.\star, 0.\star], [0.\star, \delta_\top(z, z_2)]]))$$

that maps $[a.\star, b.\star]$ to $[[a^2.\star, ab.\star], [ab.\star, b^2.\star]]$, that is $a.|0\rangle + b.|1\rangle$ to $a^2.|00\rangle + ab.|01\rangle + ab.|10\rangle + b^2.|11\rangle$ and thus expresses cloning.

References

[1] Altenkirch, T., Grattage, J., 2005. A functional quantum programming language, in: Proceedings of LICS 2005, IEEE. pp. 249–258.

[2] Arrighi, P., Dowek, G., 2017. Lineal: A linear-algebraic lambda-calculus. Logical Methods in Computer Science 13.

[3] Coecke, B., Kissinger, A., 2017. Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning. Cambridge University Press. doi:10.1017/9781316219317.

[4] Díaz-Caro, A., Dowek, G., 2019. Proof normalisation in a logic identifying isomorphic propositions, in: Geuvers, H. (Ed.), 4th International Conference on Formal Structures for Computation and Deduction (FSCD 2019), Schloss Dagstuhl– Leibniz-Zentrum fuer Informatik. pp. 14:1–14:23.

[5] Díaz-Caro, A., Guillermo, M., Miquel, A., Valiron, B., 2019. Realizability in the unitary sphere, in: Proceedings of the 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2019), pp. 1–13.

[6] Dummett, M., 1991. The Logical basis of metaphysics. Duckworth.

[7] Díaz-Caro, A., Dowek, G., Rinaldi, J., 2019. Two linearities for quantum computing in the lambda calculus. Biosystems .

[8] Gentzen, G., 1969. Untersuchungen über das logische Schliessen, in: Szabo, M. (Ed.), The Collected Papers of Gerhard Gentzen. North-Holland, pp. 68–131.

[9] Girard, J.Y., 1972. Interprétation fonctionnelle et élimination des coupures dans l'arithmétique d'ordre supérieur. Ph.D. thesis. Université de Paris 7.

[10] Jacinto, B., Read, S., 2017. General-elimination stability. Studia Logica 105, 361–405.

[11] Klop, J.W., van Oostrom, V., van Raamsdonk, F., 1993. Combinatory reduction systems: introduction and survey. Theoretical Computer Science 121, 279–308. doi:10.1016/0304-3975(93)90091-7.

[12] Mayr, R., Nipkow, T., 1998. Higher-order rewrite systems and their confluence. Theoretical Computer Science 192, 3–29. doi:10.1016/S0304-3975(97)00143-6.
[13] Miller, D., Pimentel, E., 2013. A formal framework for specifying sequent calculus proof systems. Theoretical Computer Science 474, 98–116.
[14] Miller, D., Tiu, A., 2005. A proof theory for generic judgments. ACM Transactions on Computational Logic 6, 749–783.
[15] Negri, S., von Plato, J., 2008. Structural Proof Theory. Cambridge University Press.
[16] Parigot, M., 1991. Free deduction: an analysis of computations in classical logic, in: Proceedings of Russian Conference on Logic Programming. Springer. Lecture Notes in Computer Science, pp. 361–380.
[17] Prawitz, D., 1965. Natural deduction. A proof-theoretical study. Almqvist & Wiksell.
[18] Prior, A., 1960. The runabout inference-ticket. Analysis 21, 38–39.
[19] Read, S., 2004. Identity and harmony. Analysis 64, 113–119.
[20] Read, S., 2010. General-elimination harmony and the meaning of the logical constants. Journal of Philosophical Logic 39, 557–576.
[21] Read, S., 2014. Identity and harmony revisited. https://www.st-andrews.ac.uk/~slr/identity_revisited.pdf.
[22] Schroeder-Heister, P., 1984. A natural extension of Natural deduction. The Journal of Symbolic Logic 49, 1284–1300.
[23] Selinger, P., Valiron, B., 2006. A lambda calculus for quantum computation with classical control. Mathematical Structures in Computer Science 16, 527–552.
[24] Vaux, L., 2009. The algebraic lambda calculus. Mathematical Structures in Computer Science 19, 1029–1059.
[25] Zorzi, M., 2016. On quantum lambda calculi: a foundational perspective. Mathematical Structures in Computer Science 26, 1107–1195.

Appendix A. Strong termination of proof reduction in propositional natural deduction

Definition Appendix A.1 (Syntax).

$$A = \top \mid \bot \mid A \Rightarrow A \mid A \wedge A \mid A \vee A$$
$$t = x \mid \star \mid \delta_\top(t, u) \mid \delta_\bot(t) \mid \lambda x.t \mid t\ u$$
$$\mid \langle t, u \rangle \mid \delta_\wedge^1(t, x.u) \mid \delta_\wedge^2(t, x.u)$$
$$\mid inl(t) \mid inl(r) \mid \delta_\vee(t, x.u, y.v)$$

The proofs of the form $\star$, $\lambda x.t$, $\langle t, u \rangle$, $inl(t)$, and $inr(t)$ are called *introductions*.

Definition Appendix A.2 (Typing rules).

$$\frac{}{\Gamma \vdash x : A}\ axiom\ x : A \in \Gamma$$

$$\frac{}{\Gamma \vdash \star : \top}\ \top\text{-}i$$

$$\frac{\Gamma \vdash t : \top \quad \Gamma \vdash u : C}{\Gamma \vdash \delta_\top(t, u) : C}\ \top\text{-}e$$

$$\frac{\Gamma \vdash t : \bot}{\Gamma \vdash \delta_\bot(t) : C}\ \bot\text{-}e$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \Rightarrow B}\ \Rightarrow\text{-}i$$

$$\frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash u : A}{\Gamma \vdash t\ u : B}\ \Rightarrow\text{-}e$$

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash u : B}{\Gamma \vdash \langle t, u \rangle : A \wedge B}\ \wedge\text{-}i$$

$$\frac{\Gamma \vdash t : A \wedge B \quad \Gamma, x : A \vdash u : C}{\Gamma \vdash \delta_\wedge^1(t, x.u) : C}\ \wedge\text{-}e1$$

$$\frac{\Gamma \vdash t : A \wedge B \quad \Gamma, x : B \vdash u : C}{\Gamma \vdash \delta_\wedge^2(t, x.u) : C}\ \wedge\text{-}e2$$

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

25

$$\frac{\Gamma \vdash t : B}{\Gamma \vdash inr(t) : A \vee B} \; \vee\text{-}i2$$

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

Definition Appendix A.3 (Reduction rules)**.**

$$\delta_\top(\star, v) \longrightarrow v$$
$$(\lambda x.t) \; u \longrightarrow (u/x)t$$
$$\delta_\wedge^1(\langle t, u \rangle, x.v) \longrightarrow (t/x)v$$
$$\delta_\wedge^2(\langle t, u \rangle, x.v) \longrightarrow (u/x)v$$
$$\delta_\vee(inl(t), x.v, y.w) \longrightarrow (t/x)v$$
$$\delta_\vee(inr(u), x.v, y.w) \longrightarrow (u/y)w$$

Definition Appendix A.4. *We define, by induction on the proposition A, a set of proofs $[\![A]\!]$:*

- $t \in [\![\top]\!]$ *if t strongly terminates,*

- $t \in [\![\bot]\!]$ *if t strongly terminates,*

- $t \in [\![A \Rightarrow B]\!]$ *if t strongly terminates and whenever it reduces to a proof of the form $\lambda x.u$, then for every $v \in [\![A]\!]$, $(v/x)u \in [\![B]\!]$,*

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

- $t \in [\![A \vee B]\!]$ *if t strongly terminates, whenever it reduces to a proof of the form $inl(u)$, then $u \in [\![A]\!]$, and whenever it reduces to a proof of the form $inr(v)$, then $v \in [\![B]\!]$.*

Definition Appendix A.5. *If t is a strongly terminating proof, we write $|t|$ for the maximum length of a reduction sequence issued from t.*

Proposition Appendix A.6 (Variables)**.** *For any A, the set $[\![A]\!]$ contains all the variables.*

Proof. A variable is irreducible, hence it strongly terminates. Moreover, it never reduces to an introduction. □

Proposition Appendix A.7 (Closure by reduction)**.** *If $t \in [\![A]\!]$ and $t \longrightarrow^* t'$, then $t' \in [\![A]\!]$.*

Proof. If $t \longrightarrow^* t'$ and t strongly terminates, then t' strongly terminates.

Furthermore, if A has the form $B \Rightarrow C$ and t' reduces to $\lambda x.u$, then so does t, hence for every $v \in [\![B]\!]$, $(v/x)u \in [\![C]\!]$.

If A has the form $B \wedge C$ and t' reduces to $\langle u, v \rangle$, then so does t, hence $u \in [\![B]\!]$ and $v \in [\![C]\!]$.

If A has the form $B \vee C$ and t' reduces to $inl(u)$, then so does t, hence $u \in [\![B]\!]$ and if A has the form $B \vee C$ and t' reduces to $inr(v)$, then so does t, hence $v \in [\![C]\!]$. □

Proposition Appendix A.8 (Girard's lemma)**.** *Let t be a proof that is not an introduction, such that all the one-step reducts of t are in $[\![A]\!]$. Then $t \in [\![A]\!]$.*

Proof. Let $t, t_2, ...$ be a reduction sequence issued from t. If it has a single element, it is finite. Otherwise, we have $t \longrightarrow t_2$. As $t_2 \in [\![A]\!]$, it strongly terminates and the reduction sequence is finite. Thus, t strongly terminates.

Furthermore, if A has the form $B \Rightarrow C$ and $t \longrightarrow^* \lambda x.u$, then let $t, t_2, ..., t_n$ be a reduction sequence from t to $\lambda x.u$. As t_n is an introduction and t is not, $n \geq 2$. Thus, $t \longrightarrow t_2 \longrightarrow^* t_n$. We have $t_2 \in [\![A]\!]$, thus for all $v \in [\![B]\!]$, $(v/x)u \in [\![C]\!]$.

And if A has the form $B \wedge C$ and $t \longrightarrow^* \langle u, v \rangle$, then let $t, t_2, ..., t_n$ be a reduction sequence from t to $\langle u, v \rangle$. As t_n is an introduction and t is not, $n \geq 2$. Thus, $t \longrightarrow t_2 \longrightarrow^* t_n$. We have $t_2 \in \llbracket A \rrbracket$, thus $u \in \llbracket B \rrbracket$ and $v \in \llbracket C \rrbracket$.

If A has the form $B \vee C$ and $t \longrightarrow^* inl(u)$, then let $t, t_2, ..., t_n$ be a reduction sequence from t to $inl(u)$. As t_n is an introduction and t is not, $n \geq 2$. Thus, $t \longrightarrow t_2 \longrightarrow^* t_n$. We have $t_2 \in \llbracket A \rrbracket$, thus $u \in \llbracket B \rrbracket$.

If A has the form $B \vee C$ and $t \longrightarrow^* inr(v)$, then let $t, t_2, ..., t_n$ be a reduction sequence from t to $inr(v)$. As t_n is an introduction and t is not, $n \geq 2$. Thus, $t \longrightarrow t_2 \longrightarrow^* t_n$. We have $t_2 \in \llbracket A \rrbracket$, thus $v \in \llbracket C \rrbracket$. $\square$

Proposition Appendix A.9 (Adequacy of $\star$). *We have $\star \in \llbracket \top \rrbracket$.*

Proof. As $\star$ is irreducible, it strongly terminates, hence $\star \in \llbracket \top \rrbracket$. $\square$

Proposition Appendix A.10 (Adequacy of λ). *If, for all $u \in \llbracket A \rrbracket$, $(u/x)t \in \llbracket B \rrbracket$, then $\lambda x.t \in \llbracket A \Rightarrow B \rrbracket$.*

Proof. By Proposition Appendix A.6, $x \in \llbracket A \rrbracket$, thus $t = (x/x)t \in \llbracket B \rrbracket$. Hence, t strongly terminates. Consider a reduction sequence issued from $\lambda x.t$. This sequence can only reduce t hence it is finite. Thus, $\lambda x.t$ strongly terminates.

Furthermore, if $\lambda x.t \longrightarrow^* \lambda x.t'$, then $t' \longrightarrow^* t$. Let $u \in \llbracket A \rrbracket$, $(u/x)t' \longrightarrow^* (u/x)t$, that is in $\llbracket B \rrbracket$. Hence, by Proposition Appendix A.7, $(u/x)t' \in \llbracket B \rrbracket$. $\square$

Proposition Appendix A.11 (Adequacy of $\langle, \rangle$). *If $t_1 \in \llbracket A \rrbracket$ and $t_2 \in \llbracket B \rrbracket$, then $\langle t_1, t_2 \rangle \in \llbracket A \wedge B \rrbracket$.*

Proof. The proofs t_1 and t_2 strongly terminate. Consider a reduction sequence issued from $\langle t_1, t_2 \rangle$. This sequence can only reduce t_1 and t_2, hence it is finite. Thus, $\langle t_1, t_2 \rangle$ strongly terminates.

Furthermore, if $\langle t_1, t_2 \rangle \longrightarrow^* \langle t'_1, t'_2 \rangle$, then $t'_1 \longrightarrow^* t_1$ and $t'_2 \longrightarrow^* t_2$. By Proposition Appendix A.7, $t'_1 \in \llbracket A \rrbracket$ and $t'_2 \in \llbracket B \rrbracket$. $\square$

Proposition Appendix A.12 (Adequacy of inl). *If $t \in \llbracket A \rrbracket$, then $inl(t) \in \llbracket A \vee B \rrbracket$.*

Proof. The proof t strongly terminates. Consider a reduction sequence issued from $inl(t)$. This sequence can only reduce t, hence it is finite. Thus, $inl(t)$ strongly terminates.

Furthermore, if $inl(t) \longrightarrow^* inl(t')$, then $t' \longrightarrow^* t$. By Proposition Appendix A.7, $t' \in \llbracket A \rrbracket$. And $inl(t)$ never reduces to $inr(t')$. $\square$

Proposition Appendix A.13 (Adequacy of inr). *If $t \in \llbracket B \rrbracket$, then $inr(t) \in \llbracket A \vee B \rrbracket$.*

Proof. Similar to the proof of Proposition Appendix A.12. $\square$

Proposition Appendix A.14 (Adequacy of $\delta_\top$). *If $t_1 \in \llbracket \top \rrbracket$ and $t_2 \in \llbracket C \rrbracket$, then $\delta_\top(t_1, t_2) \in \llbracket C \rrbracket$.*

Proof. The proofs t_1 and t_2 strongly terminate. We prove, by induction on $|t_1| + |t_2|$, that $\delta_\top(t_1, t_2) \in \llbracket C \rrbracket$. Using Proposition Appendix A.8, we only need to prove that every of its one step reducts is in $\llbracket C \rrbracket$. If the reduction takes place in t_1 or t_2, then we apply Proposition Appendix A.7 and the induction hypothesis.

Otherwise, the proof t_1 is $\star$ and the reduct is $t_2 \in \llbracket C \rrbracket$. $\square$

Proposition Appendix A.15 (Adequacy of $\delta_\perp$). *If $t \in \llbracket \perp \rrbracket$, then $\delta_\perp(t) \in \llbracket C \rrbracket$.*

Proof. The proof t strongly terminates. Consider a reduction sequence issued from $\delta_\perp(t)$. This sequence can only reduce t, hence it is finite. Thus, $\delta_\perp(t)$ strongly terminates. Moreover, it never reduces to an introduction. $\square$

Proposition Appendix A.16 (Adequacy of application). *If $t_1 \in \llbracket A \Rightarrow B \rrbracket$ and $t_2 \in \llbracket A \rrbracket$, then $t_1\ t_2 \in \llbracket B \rrbracket$.*

Proof. The proofs t_1 and t_2 strongly terminate. We prove, by induction on $|t_1| + |t_2|$, that $t_1\ t_2 \in \llbracket B \rrbracket$. Using Proposition Appendix A.8, we only need to prove that every of its one step reducts is in $\llbracket B \rrbracket$. If the reduction takes place in t_1 or in t_2, then we apply Proposition Appendix A.7 and the induction hypothesis.

Otherwise, the proof t_1 has the form $\lambda x.u$ and the reduct is $(t_2/x)u$. As $\lambda x.u \in \llbracket A \Rightarrow B \rrbracket$, we have $(t_2/x)u \in \llbracket B \rrbracket$. $\square$

Proposition Appendix A.17 (Adequacy of $\delta_\wedge^1$). *If $t_1 \in [\![A \wedge B]\!]$ and, for all u in $[\![A]\!]$, $(u/x)t_2 \in [\![C]\!]$, then $\delta_\wedge^1(t_1, x.t_2) \in [\![C]\!]$.*

Proof. By Proposition Appendix A.6, $x \in [\![A]\!]$ thus $t_2 = (x/x)t_2 \in [\![C]\!]$. Hence, t_1 and t_2 strongly terminate. We prove, by induction on $|t_1| + |t_2|$, that $\delta_\wedge^1(t_1, x.t_2) \in [\![C]\!]$. Using Proposition Appendix A.8, we only need to prove that every of its one step reducts is in $[\![C]\!]$. If the reduction takes place in t_1 or t_2, then we apply Proposition Appendix A.7 and the induction hypothesis.

Otherwise, the proof t_1 has the form $\langle u, v \rangle$ and the reduct is $(u/x)t_2$. As $\langle u, v \rangle \in [\![A \wedge B]\!]$, we have $u \in [\![A]\!]$. Hence, $(u/x)t_2 \in [\![C]\!]$. $\quad\square$

Proposition Appendix A.18 (Adequacy of $\delta_\wedge^2$). *If $t_1 \in [\![A \wedge B]\!]$ and, for all u in $[\![B]\!]$, $(u/x)t_2 \in [\![C]\!]$, then $\delta_\wedge^2(t_1, x.t_2) \in [\![C]\!]$.*

Proof. Similar to the proof of Proposition Appendix A.17. $\quad\square$

Proposition Appendix A.19 (Adequacy of $\delta_\vee$). *If $t_1 \in [\![A \vee B]\!]$, for all u in $[\![A]\!]$, $(u/x)t_2 \in [\![C]\!]$, and, for all v in $[\![B]\!]$, $(v/y)t_3 \in [\![C]\!]$, then $\delta_\vee(t_1, x.t_2, y.t_3) \in [\![C]\!]$.*

Proof. By Proposition Appendix A.6, $x \in [\![A]\!]$, thus $t_2 = (x/x)t_2 \in [\![C]\!]$. In the same way, $t_3 \in [\![C]\!]$. Hence, t_1, t_2, and t_3 strongly terminate. We prove, by induction on $|t_1| + |t_2| + |t_3|$, that $\delta_\vee(t_1, x.t_2, y.t_3) \in [\![C]\!]$. Using Proposition Appendix A.8, we only need to prove that every of its one step reducts is in $[\![C]\!]$. If the reduction takes place in t_1, t_2, or t_3, then we apply Proposition Appendix A.7 and the induction hypothesis. Otherwise, either:

- The proof t_1 has the form $inl(w_2)$ and the reduct is $(w_2/x)t_2$. As $inl(w_2) \in [\![A \vee B]\!]$, we have $w_2 \in [\![A]\!]$. Hence, $(w_2/x)t_2 \in [\![C]\!]$.

- The proof t_1 has the form $inr(w_3)$ and the reduct is $(w_3/x)t_3$. As $inr(w_3) \in [\![A \vee B]\!]$, we have $w_3 \in [\![B]\!]$. Hence, $(w_3/x)t_3 \in [\![C]\!]$. $\quad\square$

Theorem Appendix A.20 (Adequacy). *Let t be a proof of A in a context $\Gamma = x_1 : A_1, ..., x_n : A_n$ and σ be a substitution mapping each variable x_i to an element of $[\![A_i]\!]$, then $\sigma t \in [\![A]\!]$.*

Proof. By induction on the structure of t.

- If t is a variable, then, by definition of σ, $\sigma t \in [\![A]\!]$.

- If $t = \star$, then, by Proposition Appendix A.9, $\star \in [\![\top]\!]$, that is $\sigma t \in [\![A]\!]$.

- If $t = \lambda x.u$, where u is a proof of C, then, by induction hypothesis, for every $v \in [\![B]\!]$, $(v/x)\sigma u \in [\![C]\!]$. Hence, by Proposition Appendix A.10, $\lambda x.\sigma u \in [\![B \Rightarrow C]\!]$, that is $\sigma t \in [\![A]\!]$.

- If $t = \langle u, v \rangle$, where u is a proof of B and v a proof of C, then, by induction hypothesis, $\sigma u \in [\![B]\!]$ and $\sigma v \in [\![C]\!]$. Hence, by Proposition Appendix A.11, $\langle \sigma u, \sigma v \rangle \in [\![B \wedge C]\!]$, that is $\sigma t \in [\![A]\!]$.

- If $t = inl(u)$, where u is a proof of B, then, by induction hypothesis, $\sigma u \in [\![B]\!]$. Hence, by Proposition Appendix A.12, $inl(\sigma u) \in [\![B \vee C]\!]$, that is $\sigma t \in [\![A]\!]$.

- If $t = inr(v)$, the proof is similar, using Proposition Appendix A.13.

- If $t = \delta_\top(u, v)$, where u is a proof of $\top$ and v is a proof of A, then, by induction hypothesis, $\sigma u \in [\![\top]\!]$, and $\sigma v \in [\![A]\!]$. Hence, by Proposition Appendix A.14, $\delta_\top(\sigma u, \sigma v) \in [\![A]\!]$, that is $\sigma t \in [\![A]\!]$.

- If $t = \delta_\perp(u)$, where u is a proof of $\perp$, then, by induction hypothesis, $\sigma u \in [\![\perp]\!]$. Hence, by Proposition Appendix A.15, $\delta_\perp(\sigma u) \in [\![A]\!]$, that is $\sigma t \in [\![A]\!]$.

- If $t = u\,v$, where u is a proof of $B \Rightarrow A$ and v a proof of B, then, by induction hypothesis, $\sigma u \in [\![B \Rightarrow A]\!]$ and $\sigma v \in [\![B]\!]$. Hence, by Proposition Appendix A.16, $(\sigma u)(\sigma v) \in [\![A]\!]$, that is $\sigma t \in [\![A]\!]$.

- If $t = \delta_\wedge^1(u_1, x.u_2)$, where u_1 is a proof of $B \wedge C$ and u_2 a proof of A, then, by induction hypothesis, $\sigma u_1 \in [\![B \wedge C]\!]$, for all v in $[\![B]\!]$, $(v/x)\sigma u_2 \in [\![A]\!]$. Hence, by Proposition Appendix A.17, $\delta_\wedge^1(\sigma u_1, x.\sigma u_2) \in [\![A]\!]$, that is $\sigma t \in [\![A]\!]$.

- If $t = \delta_\wedge^2(u_1, x.u_2)$, the proof is similar, using Proposition Appendix A.18.

- If $t = \delta_\vee(u_1, x.u_2, y.u_3)$, where u_1 is a proof of $B \vee C$, u_2 a proof of A, and u_3 a proof of A, then, by induction hypothesis, $\sigma u_1 \in [\![B \vee C]\!]$, for all v in $[\![B]\!]$, $(v/x)\sigma u_2 \in [\![A]\!]$, and for all w in $[\![C]\!]$, $(w/x)\sigma u_3 \in [\![A]\!]$. Hence, by Proposition Appendix A.19, $\delta_\vee(\sigma u_1, x.\sigma u_2, y.\sigma u_3) \in [\![A]\!]$, that is $\sigma t \in [\![A]\!]$. $\qquad\square$

Corollary Appendix A.21 (Termination). *Let t be a proof of A in a context Γ. Then t strongly terminates.*

Proof. Let σ be the substitution mapping each variable $x_i : A_i$ of Γ to itself. Note that, by Proposition Appendix A.6, this variable is an element of $[\![A_i]\!]$. Then $t = \sigma t$ is an element of $[\![A]\!]$. Hence, it strongly terminates. $\qquad\square$