A Constructive Restriction of the $\lambda\mu$-calculus

Tristan Crolard

Technical Report TR-2002-02

A Constructive Restriction of
the $\lambda\mu$-calculus

Tristan Crolard*
crolard@ufr-info-p7.jussieu.fr

April 25, 1999

Abstract

We define a very natural restriction of the $\lambda\mu$-calculus which is stable under reduction and whose type system is a restriction of the Classical Natural Deduction to intuitionistic logic. However, we show that this system is in some sense degenerated unless we provide a native disjunction. We prove that the system with native disjunction is conservative over DIS-logic and also that DIS-logic is constructive. From a computational standpoint, this restriction on $\lambda\mu$-terms prevents a coroutine from accessing the local environment of another coroutine.

Keywords: type system, lambda-calculus, control operators, constructive logic.

Introduction

We define a restriction of the Classical Natural Deduction (CND), which is closed under reduction (in propositionnal, first and second order frameworks). Our first attempt results in an intuitionistic logical system which is degenerated in some sense. This defect is fixed when we supplement the system with a native disjunction. However, the resulting system is no longer conservative over intuitionistic logic but over DIS-logic (see section 1). We also show that DIS-logic is still a constructive logic.

This restriction is rephrased for the pure (i.e. untyped) $\lambda\mu$-calculus, in such a way that the former restriction is exactly the latter when we consider typed terms. We give a computational interpretation of the restriction on $\lambda\mu$-terms as "coroutines that do not access the local environment of another coroutine".

In section 2, we deal with the logical aspect of the restriction while in section 3 we consider the computational aspect and how they are both related (thanks to the Curry-Howard isomorphism).

Interpretation

Let us first recall that the definition of a catch/throw mechanism is straightforward in the $\lambda\mu$-calculus: just set **catch** $\alpha\ t \equiv \mu\alpha[\alpha]t$ and **throw** $\alpha\ t \equiv \mu\delta[\alpha]t$ where δ is a μ-variable which does not occur in t (see [3] for a study of the sublanguage obtained when we restrict the $\lambda\mu$-terms to these operators).

In $\lambda\mu$-calculus a μ-variable may be reified as the first-class continuation $\lambda x.\textbf{throw}\ \alpha\ x$. However, the type of such a $\lambda\mu$-term is the excluded-middle $\vdash A; \neg A$. Thus, continuations are no longer first-class objects in a constructive logic. This remark raises a natural question: what is the computational interpretation of our restriction on $\lambda\mu^{+}$-terms?

---

*UFR d'Informatique, Université Paris 7, 2 Place Jussieu, 75251 Paris, France

To answer this question, let us recall that first-class continuations have been sucessfully used to implement Simula-like cooperative coroutines in Scheme [28, 9]. This approach has been extended in the Standard ML of New Jersey (SML/NJ) to provide simple and elegant implementations of light-weight processes (or threads), where concurrency is obtained by having individual threads volontarily suspend themselves [25, 21, 2] (providing time-sliced processes using pre-emptive scheduling requires additional run-time system support [2, 24]).

The key point in these implementations is that control operators (such as the famous **call/cc** of Scheme and its typed counterpart **callcc** and **throw** in SML/NJ) make it possible to switch between coroutine contexts, where the context of a coroutine is just its continuation. In the restricted $\lambda\mu^+$-calculus, continuations are no longer first-class objects, but the ability of context-switching remains. However, a context is now a pair *environment + continuation* (to avoid any confusion we will call such a pair a μ-context). A μ-context is exactly what we expect as the context of a coroutine, since a coroutine should not access the local environment (the part of the environment which is not shared) of another coroutine.

Related work

The extension of the well-known formulas-as-types paradigm to classical logic has been widely investigated by T. G. Griffin [10], C. R. Murthy [14], F. Barbanera and S. Berardi [1], N. J. Rehof and M. H. Sørensen [23], P. De Groote [6], J.-L. Krivine [13], and M. Parigot [18, 19] . . .

H. Nakano, Y. Kameyama and M. Sato [16, 15, 17, 11, 12, 26] have proposed various logical frameworks that are intended to provide a type system for a lexical variant of the catch/throw mechanism used in functional languages such as Lisp. Moreover, H. Nakano has shown that it is possible to restrict the catch/throw mechanism in order to stay in an intuitionistic (propositional) framework. In this paper, we generalize H. Nakano's result in several ways:

- We use M. Parigot's $\lambda\mu$-calculus and its type system, the Classical Natural deduction (CND) [18, 19], which is confluent and strongly normalizing in the second order framework [20].

- We deal with the first and second order frameworks.

- We consider a type system *à la* Curry, which allows us to rephrase the above restriction on pure (i.e. untyped) $\lambda\mu$-terms, and not only on typed terms as in [17].

- We propose a computational interpretation of our restriction.

- On the other hand, we do not consider tag-abstraction in this paper. However, our restriction is symmetrical and thus easily extends to duality. Our purpose is to type tag-abstraction with the subtraction (the connector dual to implication). Note that subtractive logic is a conservative extension of DIS-logic [22, 5, 4].

1 DIS-logic

DIS-logic is the first order (resp. second order) intuitionistic logic extended with the following axiom schemas DIS (resp. DIS and DIS^2) where x (resp. X) does not occur in B:

$$\forall x(A \vee B) \vdash \forall x A \vee B \qquad \forall X(A \vee B) \vdash \forall X A \vee B$$

Remark. Though DIS is not valid in intuitionistic logic, if a formula $\forall x(A \vee B)$ is an intuitionistic theorem then $\forall x A \vee B$ is also an intuitionistic theorem (by the Disjunction Property).

1.1 DIS-logic is constructive

Theorem 1.1.1

- **(Disjunction Property)** *If a formula $A \vee B$ is valid in DIS-logic then either A or B is valid in DIS-logic.*

- **(Existence Property)** *If a formula $\exists x \varphi$ is valid in DIS-logic then there exists a term t such that $\varphi(t)$ is valid in DIS-logic.*

Proof. We only sketch a semantical proof of the Existence Property using Kripke models. Recall that Kripke models with constant domains are sound and complete for DIS-logic (C. Rauszer [22]). Let us first supplement the signature with an enumerable set of constants $\{c_i / i \in N\}$. We know that a formula φ with some free variables $x_1, \ldots, x_n$ is valid iff the closed formula $\varphi[c_1/x_1, \ldots, c_n/x_n]$ is valid. We will thus consider (without restriction) some closed theorem $\exists x \varphi$. We have to prove that there exists a closed term t such that $\vdash \varphi(t)$.

Let us assume that for each closed term t, we have a Kripke model $\mathcal{M}_t$ such that $\mathcal{M}_t \nVdash \varphi(t)$. Let $D(\mathcal{M})$ be the free algebra generated by the disjoint union D of the domains of all $\mathcal{M}_t$'s. Let $\mathcal{M}_t^c$ be a copy of $\mathcal{M}_t$ for each constant c that occurs in t. The domain of each $\mathcal{M}_t^c$ is extended to $D(\mathcal{M})$ in such a way that any new element is a copy of $\mathcal{M}_t(c)$. More specifically, let $\eta : D \to D(\mathcal{M}_t)$ be the mapping defined by $\eta(e) = e$ if $e \in D(\mathcal{M}_t)$ and $\eta(e) = \mathcal{M}_t(c)$ otherwise. This mapping is extended in the usual way to the free algebra $D(\mathcal{M})$. Now, for each node α of $\mathcal{M}_t^c$ and each n-ary predicate symbol P we define $\mathcal{M}(P)$ by:

$$(e_1, \ldots, e_n) \in_\alpha \mathcal{M}(P) \text{ iff } (\eta(e_1), \ldots, \eta(e_n)) \in_\alpha \mathcal{M}_t^c(P)$$

We build the model $\mathcal{M}$ by taking the disjoint union of the $\mathcal{M}_t^c$'s and adding a bottom node α_0.

Let e be an element of $D(\mathcal{M})$, let us show that $\mathcal{M} \nVdash \varphi(e)$. By definition, e has the form $t[d_1/x_1, \ldots, d_n/x_n]$ where t is a term without parameter (but with some free variables $x_1, \ldots, x_n$) and $d_1, \ldots, d_n$ are elements of D (if e is a closed term then $n = 0$). Now, let c be a constant such that for any $1 \leq i \leq n$ we have $d_i \notin D(\mathcal{M}_{\bar{t}})$ where $\bar{t}$ is the closed term $t[c/x_1, \ldots, c/x_n]$ (there are infinitely many such constants). By construction, $\mathcal{M}_{\bar{t}} \nVdash \varphi(\bar{t})$ and thus $\mathcal{M}_{\bar{t}}^c \nVdash \varphi(e)$ since for each for any $1 \leq i \leq n$, d_i is a copy of c in $\mathcal{M}_{\bar{t}}^c$. Consequently $\alpha_0 \nVdash \varphi(e)$. $\qquad\square$

2 Constructive restrictions of Classical Natural Deduction (CND)

It is well-known that if we restrict the classical sequent calculus LK [27] to sequents with at most one conclusion we obtain the intuitionistic sequent calculus LJ [27]. As for natural deduction, it was originally presented for sequents having one conclusion and formalized intuitionistic logic. Its extension to sequents with several conclusions is M. Parigot's Classical Natural Deduction [18] and leads to classical logic

When we consider a calculus with several conclusions, we would like the right comma to be a disjunction. The following definition is thus natural:

Definition 2.0.2 *We call* native disjunction *a disjunction for which the following rules are derivable:*

$$\frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B} \qquad \qquad \frac{\Gamma \vdash \Delta, A \vee B}{\Gamma \vdash \Delta, A, B}$$

Dragalin [7] and Dikhoff [8] have suggested to restrict the sole introduction rule of implication of LK to sequents with at most one conclusion. The properties of such calculus depend on the

particular rules for disjunction (and also for $\exists$ which we do not consider here). In case disjunction is second-order defined as $A \vee B \equiv \forall O(A \to O) \to (B \to O) \to O$ the rules for $\vee$ are

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B} \qquad \frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \vee B} \qquad \frac{\Gamma \vdash \Delta, A \vee B \quad \Gamma \vdash \Delta, (A \Rightarrow C) \quad \Gamma \vdash \Delta, (B \Rightarrow C)}{\Gamma \vdash \Delta, C}$$

and the calculus is degenerated. This means that for each sequent derived in such a calculus at least one conclusion is derivable under the same hypothesis.

Observe that the elimination $\vee$-rule which does not use implication (together with the introduction rules) derives and can be derived from the native rules for disjunction. Now the degeneracy phenomenon does not hold with native disjunction since then $A \vee B \vdash A, B$ is valid whereas $A \vee B \vdash A$ and $A \vee B \vdash B$ are not.

Definition 2.0.3 *We call* CND^1 *the system* CND *(with no native disjunction) where the introduction rule of implication is restricted to sequents with at most one conclusion. We call* $\mathrm{CND}^1_\vee$ *the system* CND^1 *supplemented with a native disjunction.*

Surprisingly, we have:

Proposition 2.0.4 *The system* $\mathrm{CND}^1_\vee$ *is conservative over* DIS-*logic.*

Proof. By induction on the derivation. Conversely, here is a proof of DIS in $\mathrm{CND}^1_\vee$ (the proof of DIS^2 is similar):

$$\frac{\dfrac{\dfrac{\dfrac{\dfrac{\forall x(A \vee B) \vdash \forall x(A \vee B)}{\forall x(A \vee B) \vdash A \vee B}}{\forall x(A \vee B) \vdash A, B}}{\forall x(A \vee B) \vdash \forall x A, B}}{\forall x(A \vee B) \vdash \forall x A \vee B}$$

$\square$

Remark. In the above proof, we used the introduction rule for the universal quantifier without constraint. One can check that a native disjunction with constrained $\forall$-introduction rule is conservative over intuitionistic logic.

However this restriction of the introduction rule of implication is not stable under substitution. We will thus consider a weaker restriction of CND which is stable under reduction in the next section.

2.1   A weaker restriction of CND

We use undirected links to make explicit all *interdependencies* between occurrences of hypothesis and occurrences of conclusions in any derived sequent. A link between some occurrence of an hypothesis Γ_i and some occurrence of a conclusion Δ_j may be represented as follows:

$$\Gamma_1, \ \ldots \ \overline{\Gamma_i, \ \ldots \ \Gamma_n \vdash \Delta_1, \ \ldots \ \Delta_j}, \ \ldots \ \Delta_m$$

In order to annotate sequents with such links, we name any *occurrence* of hypothesis $(x, y, z, \ldots)$ and any *occurrence* of conclusions $(\alpha, \beta, \gamma, \ldots)$ in a sequent. We assume that the name of an hypothesis (resp. a conclusion) never occurs twice in a sequent. The links annotating some sequent $\Gamma_1^{x_1}, \ldots, \Gamma_n^{x_n} \vdash \Delta_1^{\alpha_1}, \ldots, \Delta_m^{\alpha_m}$ provide a subset of $\{x_1, \ldots, x_n\} \times \{\alpha_1, \ldots, \alpha_m\}$ which can be represented by annotating either each conclusion by a set of hypothesis or each hypothesis by a set of conclusions.

Example. The sequent $A^x, B^y, C^z \vdash D^\alpha, E^\beta, F^\gamma, G^\delta$ together with the interdependencies $\{(x,\beta),(x,\delta),(z,\alpha),(z,\beta),(z,\delta)\}$ can be represented in both forms:

$$A^x, B^y, C^z \;\;\vdash\;\; \{z\}:D, \; \{x,z\}:E, \; \{\}:F, \; \{x,z\}:G$$
$$\{\beta,\delta\}{:}A, \; \{\}:B, \; \{\alpha,\beta,\delta\}:C \;\;\vdash\;\; D^\alpha, E^\beta, F^\gamma, G^\delta$$

The system $\overline{\text{CND}}$: explicit interdependencies

We will use here the former representation (*i.e.* each conclusion is annotated by a set of hypothesis). The annotations of a sequent derived in CND are defined by induction on the derivation (we omit the annotations that are not modified by the rule).

Notation. We will need the following abbreviation:

$$U[V/x] \equiv \left\{ \begin{array}{l} U\backslash\{x\} \cup V \text{ if } x \in U \\ U \text{ otherwise} \end{array} \right.$$

Axioms

$$A^x \vdash \{x\} : A$$

Weakening rule

$$\frac{\Gamma \vdash \Delta}{\Gamma, A^x \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \; \{\} : A}$$

Contraction rule

$$\frac{\Gamma, A^x, A^y \vdash S_1 : \Delta_1, \ldots, \; S_n : \Delta_n}{\Gamma, A^z \vdash S_1[z/x, z/y] : \Delta_1, \ldots, \; S_n[z/x, z/y] : \Delta_n} \qquad \frac{\Gamma \vdash \Delta, \; U : A, \; V : A}{\Gamma \vdash \Delta, \; U \cup V : A}$$

Introduction rule for $\Rightarrow$

$$\frac{\Gamma, A^x \vdash S_1 : \Delta_1, \ldots, \; S_n : \Delta_n, \; V : B}{\Gamma \vdash S_1 \backslash \{x\} : \Delta_1, \ldots, \; S_n \backslash \{x\} : \Delta_n, \; V \backslash \{x\} : (A \Rightarrow B)}$$

Elimination rule for $\Rightarrow$

$$\frac{\Gamma \vdash \Delta, \; U : (A \Rightarrow B) \qquad \Gamma' \vdash \Delta', \; V : A}{\Gamma, \Gamma' \vdash \Delta, \Delta', \; U \cup V : B}$$

Remark. If an hypothesis (resp. a conclusion) occurs with the same name in Γ and Γ' (resp. in Δ and Δ') then these occurrences are implicitly contracted using the left (resp. right) contraction rule. Thus the name of an hypothesis (resp. a conclusion) never occurs twice in a sequent. To allow multiplicatives rules we should consider a new kind of weakening rules, which add a link between an hypothesis and a conclusion as follows:

$$\frac{\Gamma_1, \ldots, \; \Gamma_i^{x_i}, \ldots, \Gamma_n \vdash \Delta_1, \ldots, \; S_j : \Delta_j, \ldots, \Delta_p}{\Gamma_1, \ldots, \; \Gamma_i^{x_i}, \ldots, \Gamma_n \vdash \Delta_1, \ldots, \; S_j \cup \{x_i\} : \Delta_j, \ldots, \Delta_p}$$

Cut rule

$$\frac{\Gamma \vdash S_1 : \Delta_1, \ldots, \ S_n : \Delta_n, \ S : A \qquad \Gamma', A^x \vdash S'_1 : \Delta'_1, \ldots, \ S'_p : \Delta'_p}{\Gamma, \Gamma' \vdash S_1 : \Delta_1, \ldots, \ S_n : \Delta_n, \ S'_1[S/x] : \Delta'_1, \ldots, \ S'_p[S/x] : \Delta'_p}$$

Remark. If we consider the rules for which a left/right symmetry holds (contraction and weakening) we notice that annotations are also symmetrical to one another. For instance, the left contraction rule might have been annotated as follows (where this time hyphotesis are annoted):

$$\frac{\Gamma, \ U : A, \ V : A \vdash \Delta}{\Gamma, \ U \cup V : A \vdash \Delta}$$

Intro. rule (if x does not occur in Γ, Δ) **and elim. rule for** $\forall$

(idem for $\forall^2$)

$$\frac{\Gamma \vdash \Delta, \ S : A}{\Gamma \vdash \Delta, \ S : \forall x A} \qquad\qquad \frac{\Gamma \vdash \Delta, \ S : \forall x A}{\Gamma \vdash \Delta, \ S : A[t/x]}$$

Intro. rule (if x does not occur in Γ, Δ) **and elim rule for** $\forall^2$

$$\frac{\Gamma \vdash \Delta, \ S : A}{\Gamma \vdash \Delta, \ S : \forall X A} \qquad\qquad \frac{\Gamma \vdash \Delta, \ S : \forall X A}{\Gamma \vdash \Delta, \ S : A[T/X]}$$

Notation. We denote $\overline{\text{CND}}$ the system CND where interdependencies are explicit.

Remark. Any proof of CND is a proof of $\overline{\text{CND}}$, it suffices to annotate the proof.

Definition 2.1.1 *In* $\overline{\text{CND}}$, *an instance of the introduction rule of implication is* constructive *iff x does not occur in any S_i. The rule becomes then:*

$$\frac{\Gamma, A^x \vdash S_1 : \Delta_1, \ldots, \ S_n : \Delta_n, \ V : B}{\Gamma \vdash S_1 : \Delta_1, \ldots, \ S_n : \Delta_n, \ V \setminus \{x\} : (A \Rightarrow B)} \quad \text{where } x \notin S_1 \cup \ldots \cup S_n$$

In other words, to stay in a constructive framework, an hypothesis may be discharged over some conclusion if and only if no other conclusion depends on it. This constraint extends to proofs:

Definition 2.1.2 *A proof of* $\overline{\text{CND}}$ *is said to be* constructive *if any occurrence of the introduction rule of implication is* constructive. *We call* $\overline{\text{CND}}^r$ *the restriction of* $\overline{\text{CND}}$ *to constructive proofs.*

Remark. Any proof of CND[1] is obviously a proof of $\overline{\text{CND}}^r$.

The following theorem say that $\overline{\text{CND}}^r$ (and thus also CND[1]) is degenerated in some way.

Theorem 2.1.3 *For any sequent* $\Gamma \vdash \Delta$ *derived in* $\overline{\text{CND}}^r$, *then* $\Sigma \vdash \Delta_j$ *is valid in intuitionistic logic for at least one* Δ_j. *More specifically, if* Σ *is the subset of hypothesis of* Γ *which are linked to* Δ_j *in the sequent* $\Gamma \vdash \Delta$, *then* $\Sigma \vdash \Delta_j$ *is valid in intuitionistic logic.*

Proof. Let us show than any conclusion Δ_j which does not come, directly or indirectly, from an occurence of the weakening rule satisfies the property stated in the theorem. In order to emphasize these conclusions which come from an occurence of the weakening rule, we will add a new kind of annotation for conclusions: the *symbol* ∞. The right-hand weakening and contraction rules thus become:

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \ \infty : B} \qquad\qquad \frac{\Gamma \vdash \Delta, \ U : B, \ V : B}{\Gamma \vdash \Delta, \ W : B}$$

where W is defined as follows:

6

- $W = \infty$ if $U = \infty$ and $V = \infty$

- $W = V$ if $U = \infty$ and $V \neq \infty$

- $W = U$ if $U \neq \infty$ and $V = \infty$

- $W = V$ or $W = U$ if $U \neq \infty$ and $V \neq \infty$

In the last case, two annotations are possible: this process of extraction is thus intrinsically non deterministic.

We now extend the set-theroretic operations used to define the previous annotations to this new symbol in the following way:

- $U \cup \infty = \infty \cup U = \infty$

- $\infty \backslash \{x\} = \infty$

- $\infty[U/x] = \infty$

- $U[\infty/x] = \infty$, if x occurs in U and $U[\infty/x] = U$ otherwise

If Γ is the set of hypothesis $\Gamma^{x_1}, \dots, \Gamma^{x_n}$ and S is a subset of $\{x_1, \dots, x_n\}$, we denote Γ^S the subset of hypothesis of Γ whose name occur in S. We check then by recurrence on the proof that, for any derived sequent $\Gamma \vdash \Delta$, on the one hand, there exists at least one conclusion which is not annotated by ∞, and on the other hand, for any conclusion Δ_j annotated by some (possibly empty) set S of hypothesis names, $\Gamma^S \vdash_{\mathrm{NJ}} \Delta_j$.

The only tricky case is the implication's introduction rule. By definition, an occurrence of this rule:

$$\frac{\Gamma, A^x \vdash V : B, \ S_1 : \Delta_1, \dots, \ S_n : \Delta_n}{\Gamma \vdash V \backslash \{x\} : (A \Rightarrow B), \ S_1 \backslash \{x\} : \Delta_1, \dots, \ S_n \backslash \{x\} : \Delta_N}$$

is intuitionistic if, for any conclusion Δ_j annotated by S_j we have either $S_j = \infty$ or S_j is a set of hypothesis names such as $x \notin S_j$. In the latter case, by recurrence hypothesis, we have $\Gamma^{S_j} \vdash_{\mathrm{NJ}} \Delta_j$ and consequently, $\Gamma^{S_j \backslash \{x\}} \vdash_{\mathrm{NJ}} \Delta_j$ since $S_j \backslash \{x\} = S_j$. Now, if $V \neq \infty$ then by recurrence hypothesis, $\Gamma^V \vdash_{\mathrm{NJ}} B$ hence $\Gamma^{V \backslash \{x\}} \vdash_{\mathrm{NJ}} A \Rightarrow B$. If $V = \infty$ then there exists at least one conclusion Δ_j which is not annotated by ∞ and such as $\Gamma^{S_j} \vdash_{\mathrm{NJ}} \Delta_j$. $\qquad \square$

Remark. If we define $A \wedge B$ as the second order formula $A \wedge B \equiv \forall O(A \to B \to O) \to O$, it is easy to derive the following annotated rules for $\wedge$:

$$\frac{\Gamma \vdash \Delta, U : A \quad \Gamma \vdash \Delta, V : B}{\Gamma \vdash \Delta, U \cup V : A \wedge B} \qquad \frac{\Gamma \vdash \Delta, S : A \wedge B}{\Gamma \vdash \Delta, S : A} \qquad \frac{\Gamma \vdash \Delta, S : A \wedge B}{\Gamma \vdash \Delta, S : B}$$

2.2 Native disjunction

The usual definition of $A \vee B$ as the second order formula $\equiv \forall O(A \to O) \to (B \to O) \to O$ allow us to derive the following annotated rules for $\vee$:

$$\frac{\Gamma \vdash \Delta, S : A}{\Gamma \vdash \Delta, S : A \vee B} \qquad \frac{\Gamma \vdash \Delta, S : B}{\Gamma \vdash \Delta, S : A \vee B}$$

$$\frac{\Gamma \vdash \Delta, U : A \vee B \quad \Gamma \vdash \Delta, V : (A \Rightarrow C) \quad \Gamma \vdash \Delta, W : (B \Rightarrow C)}{\Gamma \vdash \Delta, U \cup V \cup W : C}$$

Yet, with these rules defining the disjunction, by the theorem 2.1.3, we are not able to derive the sequent $A \vee B \vdash A, B$ since clearly neither the sequent $A \vee B \vdash A$ nor the sequent $A \vee B \vdash B$ is valid in intuitionistic logic.

It is easy to derive the annotated rules of a native disjunction by symmetry. The left introduction rule of $\vee$ which is dual to the right introduction rule of $\wedge$ (where hypothesis are annotated):

$$\frac{\Gamma, \, U:A \vdash \Delta \qquad \Gamma, \, V:B \vdash \Delta}{\Gamma, \, U \cup V : A \vee B \vdash \Delta}$$

Let us annotate this rule on the right-hand side:

$$\frac{\Gamma, A^x \vdash S_1:\Delta_1, \dots, \, S_n:\Delta_n, \qquad \Gamma', B^y \vdash S_1':\Delta_1', \dots, \, S_p':\Delta_p'}{\Gamma, \Gamma', A \vee B^z \vdash S_1[z/x]:\Delta_1, \dots, \, S_n[z/x]:\Delta_n, \, S_1'[z/x]:\Delta_1', \dots, \, S_p'[z/x]:\Delta_p'}$$

Using the cut rule, we eventually obtain the right-hand annotations for the usual (in natural deduction style) elimination rule of disjunction. The introduction rules are easier to derive. We sum up these rules in the following definition:

Definition 2.2.1 *We call $\overline{\mathrm{CND}}_\vee^r$ the calculus $\overline{\mathrm{CND}}^r$ supplemented by a native disjunction, denoted $\vee$, and defined by the following rules:*

$$\frac{\Gamma \vdash \Delta; S:A}{\Gamma \vdash \Delta; S:A \vee B} \qquad \frac{\Gamma \vdash \Delta; S:B}{\Gamma \vdash \Delta; S:A \vee B}$$

$$\frac{\Gamma \vdash \Delta, S:A \vee B \qquad \Gamma, A^x \vdash S_1:\Delta_1, \dots, \, S_n:\Delta_n \qquad \Gamma', B^y \vdash S_1':\Delta_1', \dots, \, S_p':\Delta_p'}{\Gamma, \Gamma', \Gamma'' \vdash \Delta, S_1[S/x]:\Delta_1, \dots, \, S_n[S/x]:\Delta_n, \, S_1'[S/y]:\Delta_1', \dots, \, S_p'[S/y]:\Delta_p'}$$

Theorem 2.2.2 *A sequent is derivable in $\overline{\mathrm{CND}}_\vee^r$ iff it is valid in DIS-logic (in the first and second order frameworks).*

Proof. (sketch) First an easy induction on derivations shows that any sequent derivable in $\mathrm{CND}_\vee$ from sequents valid in DIS-logic without the introduction rule of implication is also valid in DIS-logic. Another induction shows that a proof of a sequent in $\overline{\mathrm{CND}}_\vee^r$ can be turned into a proof of the same sequent using axioms valid in DIS-logic but whithout any occurrence of the constructive introduction rule of implication (the details of the proof are given in appendix A.1). Whence this sequent is valid in DIS-logic. $\qquad \square$

3 The typed $\lambda\mu^+$-calculus

Parigot [18] introduced the $\lambda\mu^+$-calculus which allows for a Curry-Howard correspondance with the Classical Natural Deduction. Here we consider the $\lambda\mu$-calculus, with injections **inl** and **inr**, **cases** and **let** instructions which we call $\lambda\mu^+$-calculus. We recall the syntax of this calculus and give the definition of a $\lambda\mu^+$-term safe with respect to μ-contexts (μ-safe for short): this is a formal definition of a $\lambda\mu$-term in which a coroutine does not access any local variable of another coroutine. We show that this restriction is stable under the reduction rules of the $\lambda\mu^+$-calculus. By construction, μ-safe $\lambda\mu^+$-terms and proofs of $\overline{\mathrm{CND}}_\vee^r$ are related by the following statement: given the derivation of a type judgement of a $\lambda\mu^+$-term t by some sequent in $\overline{\mathrm{CND}}_\vee$, if t is μ-safe then this derivation belongs to $\overline{\mathrm{CND}}_\vee^r$ (and the sequent is valid in DIS-logic).

3.1 The $\lambda\mu^+$-calculus

As usual, we denote λ-variables $x, y, z \ldots$ and μ-variables $\alpha, \beta, \gamma \ldots$

Definition 3.1.1 *If t, u, v are $\lambda\mu^+$-terms then*

$$x, \ (u\ v), \ \lambda x.t, \ \mu\alpha[\beta]t, \ \textbf{inl } t, \ \textbf{inr } t, \ \textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v, \ \textbf{let } x = t \textbf{ in } u$$

are also $\lambda\mu^+$-terms.

Reduction rules of the $\lambda\mu^+$-calculus

1. $(\lambda x.u\ v) \rightsquigarrow u\{v/x\}$

2. $(\mu\alpha u\ v) \rightsquigarrow \mu\alpha u\{[\alpha](t\ v)/[\alpha]t\}$

3. $[\beta]\mu\alpha t \rightsquigarrow t\{\beta/\alpha\}$

4. $\mu\alpha[\alpha]t \rightsquigarrow t$ if α does not occur free in t.

5. $\textbf{let } x = u \textbf{ in } t \rightsquigarrow t\{u/x\}$

6. $\textbf{cases } (\textbf{inl } t) \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v \rightsquigarrow u\{t/x\}$

7. $\textbf{cases } (\textbf{inr } t) \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v \rightsquigarrow v\{t/y\}$

8. $\textbf{cases } \mu\alpha w \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v \rightsquigarrow \mu\alpha w\{[\alpha]\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v)/[\alpha]t\}$

The notation $u\{v/x\}$ stands for the usual substitution of the λ-variable x by v in u. The notation $u\{[\alpha]v/[\alpha]t\}$ means "replace in the term u term any occurrence of any subterm of the form $[\alpha]t$ by $[\alpha]v$".

Remark. The $\lambda\mu$-calculus is strongly normalizing in the second order framework. This result can be easily extended to the $\lambda\mu^+$-calculus using the definition of the disjunction as a second order formula and **cases**, **inl**, **inr**, **let** as macros:

- $\textbf{let } x = u \textbf{ in } t \equiv (\lambda x.t\ u)$

- $\textbf{inl } t \equiv \lambda f \lambda g(f\ t)$

- $\textbf{inr } t \equiv \lambda f \lambda g(g\ t)$

- $\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v \equiv (t\ \lambda x.u\ \lambda y.v)$

If we denote Φ the previous translation from the $\lambda\mu^+$-calculus into the $\lambda\mu$-calculus, it is easy to check the following properties:

1. Φ is a morphism for the reduction: if $u \rightsquigarrow_{\lambda\mu^+} v$ then $\Phi(u) \rightsquigarrow_{\lambda\mu}^n \Phi(v)$ (with $n > 0$)

2. Φ preserves normal forms: if u is a normal $\lambda\mu^+$-term then $\Phi(u)$ is a normal $\lambda\mu$-term.

From the first property, we can derive the strong normalization of the second order $\lambda\mu^+$-calculus, and from the second property, the uniqueness of the normal form (but not the Church-Rosser property). We also know that we have enough rules to obtain "good normal forms" (since they are the same as in the $\lambda\mu$-calculus).

3.2 Typing rules

Axiom

$$x : A^x \vdash A$$

Rules of →

$$\frac{t : \Gamma, A^x \vdash \Delta; B}{\lambda x.t : \Gamma \vdash \Delta; A \rightarrow B} \qquad \frac{u : \Gamma \vdash \Delta; A \rightarrow B \qquad v : \Gamma \vdash \Delta; A}{(u\ v) : \Gamma \vdash \Delta; B}$$

Rules of ∀

$$\frac{u : \Gamma \vdash \Delta; A}{u : \Gamma \vdash \Delta; \forall x A} \qquad \frac{u : \Gamma \vdash \Delta; \forall x A}{u : \Gamma \vdash \Delta; A\{t/x\}}$$

Rules of ∀²

$$\frac{u : \Gamma \vdash \Delta; A}{u : \Gamma \vdash \Delta; \forall X A} \qquad \frac{u : \Gamma \vdash \Delta; \forall X A}{u : \Gamma \vdash \Delta; A\{T/X\}}$$

Naming rules

$$\frac{t : \Gamma \vdash \Delta; A}{[\alpha]t : \Gamma \vdash \Delta, A^\alpha;} \qquad \frac{t : \Gamma \vdash \Delta, A^\alpha;}{\mu\alpha.t : \Gamma \vdash \Delta; A}$$

Rules of ∨

$$\frac{t : \Gamma \vdash \Delta, A}{\mathbf{inl}\ t : \Gamma \vdash \Delta, A \vee B} \qquad \frac{t : \Gamma \vdash \Delta, B}{\mathbf{inr}\ t : \Gamma \vdash \Delta, A \vee B}$$

$$\frac{t : \Gamma \vdash \Delta, A \vee B \qquad u : \Gamma, A^x \vdash \Delta, C \qquad v : \Gamma, B^y \vdash \Delta, C}{\mathbf{cases}\ t\ \mathbf{of}\ (\mathbf{inl}\ x) \mapsto u \mid (\mathbf{inr}\ y) \mapsto v : \Gamma \vdash \Delta, C}$$

Cut rule

$$\frac{u : \Gamma \vdash \Delta; A \qquad t : \Gamma, A^x \vdash \Delta; B}{\mathbf{let}\ x = u\ \mathbf{in}\ t : \Gamma \vdash \Delta; B}$$

3.3 Scope of a μ-variable

In this section we introduce the concept of scope of a μ-variable with respect to λ-variables. This leads to the formal definition of a $\lambda\mu^+$-term in which a coroutine does not access any local variable of another coroutine. We will say that such a $\lambda\mu^+$-term is *safe with respect to μ-contexts*.

Definition 3.3.1 *We define by induction on t the set $\mathcal{S}_{[]}(t)$ of the free λ-variables that occur* out *of the scope of any μ-variable in t and the set $\mathcal{S}_\delta(t)$ of the free λ-variables that occur* in *the scope of a free μ-variable δ in t:*

- $\mathcal{S}_{[]}(x) = \{x\}$
  $\mathcal{S}_\delta(x) = \emptyset$

- $\mathcal{S}_{[]}(\lambda x.u) = \mathcal{S}_{[]}(u)\backslash\{x\}$
  $\mathcal{S}_{\delta}(\lambda x.u) = \mathcal{S}_{\delta}(u)\backslash\{x\}$

- $\mathcal{S}_{[]}(u\ v) = \mathcal{S}_{[]}(u) \cup \mathcal{S}_{[]}(v)$
  $\mathcal{S}_{\delta}(u\ v) = \mathcal{S}_{\delta}(u) \cup \mathcal{S}_{\delta}(v)$

- $\mathcal{S}_{[]}([\alpha]u) = \emptyset$
  $\mathcal{S}_{\delta}([\alpha]u) = \mathcal{S}_{\delta}(u)$ *for any* $\delta \neq \alpha$ *and* $\mathcal{S}_{\alpha}([\alpha]u) = \mathcal{S}_{\alpha}(u) \cup \mathcal{S}_{[]}(u)$

- $\mathcal{S}_{[]}(\mu\alpha.u) = \mathcal{S}_{\alpha}(u)$
  $\mathcal{S}_{\delta}(\mu\alpha.u) = \mathcal{S}_{\delta}(u)$

- $\mathcal{S}_{[]}(\mathbf{inl}\ u) = \mathcal{S}_{[]}(u)$ *and* $\mathcal{S}_{[]}(\mathbf{inr}\ u) = \mathcal{S}_{[]}(u)$
  $\mathcal{S}_{\delta}(\mathbf{inl}\ u) = \mathcal{S}_{\delta}(u)$ *and* $\mathcal{S}_{\delta}(\mathbf{inr}\ u) = \mathcal{S}_{\delta}(u)$

- $\mathcal{S}_{[]}(\mathbf{cases}\ w\ \mathbf{of}\ (\mathbf{inl}\ x) \mapsto u\ |\ (\mathbf{inr}\ y) \mapsto v) = \mathcal{S}_{[]}(u)[\mathcal{S}_{[]}(w)/x] \cup \mathcal{S}_{[]}(v)[\mathcal{S}_{[]}(w)/y]$
  $\mathcal{S}_{\delta}(\mathbf{cases}\ w\ \mathbf{of}\ (\mathbf{inl}\ x) \mapsto u\ |\ (\mathbf{inr}\ y) \mapsto v) = \mathcal{S}_{\delta}(u)[\mathcal{S}_{[]}(w)/x] \cup \mathcal{S}_{\delta}(v)[\mathcal{S}_{[]}(w)/y] \cup \mathcal{S}_{\delta}(w)$

- $\mathcal{S}_{[]}(\mathbf{let}\ x = v\ \mathbf{in}\ u) = \mathcal{S}_{[]}(u)[\mathcal{S}_{[]}(v)/x]$
  $\mathcal{S}_{\delta}(\mathbf{let}\ x = v\ \mathbf{in}\ u) = \mathcal{S}_{\delta}(u)[\mathcal{S}_{[]}(v)/x] \cup \mathcal{S}_{\delta}(v)$

Remark. In the particular case of $\lambda\mu\mathbf{ct}$-terms, the previous definition may be rephrased as follows:

- If the $\lambda\mu\mathbf{ct}$-term is **catch** $\alpha\ u$ (i.e. $\mu\alpha[\alpha]u$) then:
  $\mathcal{S}_{[]}(\mu\alpha[\alpha]u) = \mathcal{S}_{\alpha}([\alpha]u) = \mathcal{S}_{[]}(u) \cup \mathcal{S}_{\alpha}(u)$
  $\mathcal{S}_{\delta}(\mu\alpha[\alpha]u) = \mathcal{S}_{\delta}([\alpha]u) = \mathcal{S}_{\delta}(u)$

- If the $\lambda\mu\mathbf{ct}$-term is **throw** $\alpha\ u$ (i.e. $\mu\beta[\alpha]u$ where β does not occur in $[\alpha]u$) then:
  $\mathcal{S}_{[]}(\mu\beta[\alpha]u) = \mathcal{S}_{\beta}([\alpha]u) = \emptyset$
  $\mathcal{S}_{\delta}(\mu\beta[\alpha]u) = \mathcal{S}_{\delta}([\alpha]u) = \mathcal{S}_{\delta}(u)$ for any $\delta \neq \alpha$ and $\mathcal{S}_{\alpha}(\mu\beta[\alpha]u) = \mathcal{S}_{\alpha}([\alpha]u) = \mathcal{S}_{\alpha}(u) \cup \mathcal{S}_{[]}(u)$

Remark. Given a $\lambda\mu^+$-term t, a λ-variable may occur out of the scope of any free μ-variable in t *and also* in the scope of *several* free μ-variables in t. Such a λ-variable is *shared* between several coroutines and the current routine.

Definition 3.3.2 *A* $\lambda\mu^+$*-term* t *is* safe with respect to μ-contexts (μ-safe *for short) iff for any subterm of* t *which has the form* $\lambda x.u$*, for any free* μ*-variable* δ *of* u*,* $x \notin \mathcal{S}_{\delta}(u)$ *.*

Remark. In μ-safe $\lambda\mu^+$-terms, the usual abbreviation $(\lambda x.t\ u)$ is no longer equivalent to **let** $x = u$ **in** t since in $(\lambda x.t\ u)$, the λ-variable x may not occur in the scope of some μ-variable in t: this declaration of x is local to the current routine.

3.4   Closure under reduction

In this section, we prove that the subset of μ-safe $\lambda\mu^+$-terms is closed under the reduction rules of the $\lambda\mu^+$-calculus.

Lemma 3.4.1 $\mathcal{S}_{\delta}(t) = \emptyset$ *if* δ *does not occur in* t*.*

Lemma 3.4.2 *If* u *and* v *are* $\lambda\mu^+$*-terms then:*

$$\mathcal{S}_{[]}(u\{v/x\}) \subseteq \mathcal{S}_{[]}(u)[\mathcal{S}_{[]}(v)/x]$$
$$\mathcal{S}_{\delta}(u\{v/x\}) \subseteq \mathcal{S}_{\delta}(u)[\mathcal{S}_{[]}(v)/x] \cup \mathcal{S}_{\delta}(v)$$

Lemma 3.4.3 *If t is a $\lambda\mu^+$-term then:*

$$\begin{aligned}
\mathcal{S}_{[]}(t\{\beta/\alpha\}) &\subseteq \mathcal{S}_{[]}(t) \\
\mathcal{S}_{\beta}(t\{\beta/\alpha\}) &\subseteq \mathcal{S}_{\beta}(t) \cup \mathcal{S}_{\alpha}(t) \\
\mathcal{S}_{\delta}(t\{\beta/\alpha\}) &\subseteq \mathcal{S}_{\delta}(t) \text{ for any } \delta \neq \beta
\end{aligned}$$

Lemma 3.4.4 *If t and v are $\lambda\mu^+$-terms such that α does not occur in v then:*

$$\begin{aligned}
\mathcal{S}_{[]}(t\{[\alpha](u\ v)/[\alpha]u\}) &\subseteq \mathcal{S}_{[]}(t) \\
\mathcal{S}_{\alpha}(t\{[\alpha](u\ v)/[\alpha]u\}) &\subseteq \mathcal{S}_{\alpha}(t) \cup \mathcal{S}_{[]}(v) \\
\mathcal{S}_{\delta}(t\{[\alpha](u\ v)/[\alpha]u\}) &\subseteq \mathcal{S}_{\delta}(t) \cup \mathcal{S}_{\delta}(v) \text{ for any } \delta \neq \alpha
\end{aligned}$$

Lemma 3.4.5 *If u, v, w are $\lambda\mu^+$-terms such that α does not occur in u, v then:*

$$\begin{aligned}
\mathcal{S}_{[]}(w\{[\alpha]\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v)/[\alpha]t\}) &\subseteq \mathcal{S}_{[]}(w) \\
\mathcal{S}_{\alpha}(w\{[\alpha]\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v)/[\alpha]t\}) &\subseteq \mathcal{S}_{[]}(u)[\mathcal{S}_{\alpha}(w)/x] \cup \mathcal{S}_{[]}(v)[\mathcal{S}_{\alpha}(w)/y] \\
\mathcal{S}_{\delta}(w\{[\alpha]\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v)/[\alpha]t\}) &\subseteq \mathcal{S}_{\delta}(u)[\mathcal{S}_{\alpha}(w)/x] \cup \mathcal{S}_{\delta}(v)[\mathcal{S}_{\alpha}(w)/y] \cup \mathcal{S}_{\delta}(w) \\
&\qquad \text{for any } \delta \neq \alpha
\end{aligned}$$

Lemma 3.4.6 *Given an instance $r \rightsquigarrow s$ of a rule of the $\lambda\mu^+$-calculus, if r is μ-safe then $\mathcal{S}_{[]}(s) \subseteq \mathcal{S}_{[]}(r)$ and $\mathcal{S}_{\delta}(s) \subseteq \mathcal{S}_{\delta}(r)$ for any a free μ-variable δ of s.*

Proof. Let us consider each reduction rule of the $\lambda\mu^+$-calculus. Let y be a free λ-variable of s (and thus a free λ-variable of r) and let δ be a free μ-variable δ in s (and thus a free μ-variable δ in r):

- $r = (\lambda x.u\ v)$ and $s = u\{v/x\}$. By lemma 3.4.2:

  $\mathcal{S}_{[]}(u\{v/x\}) \subseteq \mathcal{S}_{[]}(u)[\mathcal{S}_{[]}(v)/x] \subseteq \mathcal{S}_{[]}(u)\backslash\{x\} \cup \mathcal{S}_{[]}(v) = \mathcal{S}_{[]}(\lambda x.u\ v)$

  $\mathcal{S}_{\delta}(u\{v/x\}) \subseteq \mathcal{S}_{\delta}(u)[\mathcal{S}_{[]}(v)/x] \cup \mathcal{S}_{\delta}(v) \subseteq \mathcal{S}_{\delta}(u)\backslash\{x\} \cup \mathcal{S}_{\delta}(v) = \mathcal{S}_{\delta}(\lambda x.u\ v)$ (since r is μ-safe and thus $x \notin \mathcal{S}_{\delta}(u)$)

- $r = (\mu\alpha.t\ v)$ and $s = \mu\alpha.t\{[\alpha](u\ v)/[\alpha]u\}$. By lemma 3.4.4:

  $\mathcal{S}_{[]}(\mu\alpha.t\{[\alpha](u\ v)/[\alpha]u\}) \subseteq \mathcal{S}_{\alpha}(t\{[\alpha](u\ v)/[\alpha]u\}) \cup \mathcal{S}_{[]}(t\{[\alpha](u\ v)/[\alpha]u\}) \subseteq \mathcal{S}_{\alpha}(t) \cup \mathcal{S}_{\alpha}(v) \cup \mathcal{S}_{[]}(t) = \mathcal{S}_{\alpha}(\mu\alpha.t\ v)$

  $\mathcal{S}_{\delta}(\mu\alpha.t\{[\alpha](u\ v)/[\alpha]u\}) \subseteq \mathcal{S}_{\delta}(t\{[\alpha](u\ v)/[\alpha]u\}) \subseteq \mathcal{S}_{\delta}(t) \cup \mathcal{S}_{\delta}(v) = \mathcal{S}_{\delta}(\mu\alpha.t\ v)$

- $r = [\beta]\mu\alpha.t$ and $s = t\{\beta/\alpha\}$. By lemma 3.4.3:

  $\mathcal{S}_{[]}(t\{\beta/\alpha\}) \subseteq \mathcal{S}_{[]}(t) = \emptyset = \mathcal{S}_{\alpha}([\beta]\mu\alpha.t)$ (since t has the form $[\delta]v$)

  $\mathcal{S}_{\beta}(t\{\beta/\alpha\}) \subseteq \mathcal{S}_{\beta}(t) \cup \mathcal{S}_{\alpha}(t) = \mathcal{S}_{\beta}(\mu\alpha.t) \cup \mathcal{S}_{[]}(\mu\alpha.t) = \mathcal{S}_{\beta}([\beta]\mu\alpha.t)$

  $\mathcal{S}_{\delta}(t\{\beta/\alpha\}) \subseteq \mathcal{S}_{\delta}(t) = \mathcal{S}_{\delta}(\mu\alpha.t) = \mathcal{S}_{\delta}([\beta]\mu\alpha.t)$ for any $\delta \neq \beta$

- $r = \mu\alpha[\alpha]u$ and $s = u$ where α does not occur free in u.

  $\mathcal{S}_{[]}(u) = \mathcal{S}_{[]}(u) \cup \mathcal{S}_{\alpha}(u) = \mathcal{S}_{\alpha}([\alpha]u) = \mathcal{S}_{[]}(\mu\alpha[\alpha]u)$ (since $\mathcal{S}_{\alpha}(u) = \emptyset$)

  $\mathcal{S}_{\delta}(u) = \mathcal{S}_{\delta}([\alpha]u) = \mathcal{S}_{\delta}(\mu\alpha[\alpha]u)$

- $r = \textbf{let } x = u \textbf{ in } t$ and $s = t\{u/x\}$. By lemma 3.4.2:

  $\mathcal{S}_{[]}(t\{u/x\}) \subseteq \mathcal{S}_{[]}(t)[\mathcal{S}_{[]}(u)/x] = \mathcal{S}_{[]}(\textbf{let } x = u \textbf{ in } t)$

  $\mathcal{S}_{\delta}(t\{u/x\}) \subseteq \mathcal{S}_{\delta}(t)[\mathcal{S}_{[]}(u)/x] \cup \mathcal{S}_{\delta}(v) = \mathcal{S}_{\delta}(\textbf{let } x = u \textbf{ in } t)$

- $r = \textbf{cases } (\textbf{inl } t) \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v$ and $s = u\{t/x\}$

  $\mathcal{S}_{[]}(u\{t/x\}) \subseteq \mathcal{S}_{[]}(u)[\mathcal{S}_{[]}(t)/x] \subseteq \mathcal{S}_{[]}(u)[\mathcal{S}_{[]}(t)/x] \cup \mathcal{S}_{[]}(v)[\mathcal{S}_{[]}(t)/y] = \mathcal{S}_{[]}(r)$

  $\mathcal{S}_{\delta}(u\{t/x\}) \subseteq \mathcal{S}_{\delta}(u)[\mathcal{S}_{[]}(t)/x] \cup \mathcal{S}_{\delta}(t) \subseteq \mathcal{S}_{\delta}(u)[\mathcal{S}_{[]}(t)/x] \cup \mathcal{S}_{\delta}(v)[\mathcal{S}_{[]}(t)/y] \cup \mathcal{S}_{\delta}(t) = \mathcal{S}_{[]}(r)$

- $r = \textbf{cases } \mu\alpha w \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v$

  and $s = \mu\alpha w\{[\alpha]\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v)/[\alpha]t\}$, By lemma 3.4.5:

  $\mathcal{S}_{[]}(\mu\alpha w\{[\alpha]\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v)/[\alpha]t\})$

  $\qquad = \mathcal{S}_{\alpha}(w\{[\alpha]\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v)/[\alpha]t\})$

  $\qquad \subseteq \mathcal{S}_{[]}(u)[\mathcal{S}_{\alpha}(w)/x] \cup \mathcal{S}_{[]}(v)[\mathcal{S}_{\alpha}(w)/y]$

  $\qquad = \mathcal{S}_{[]}(u)[\mathcal{S}_{[]}(\mu\alpha w)/x] \cup \mathcal{S}_{[]}(v)[\mathcal{S}_{[]}(\mu\alpha w)/y] = \mathcal{S}_{[]}(r)$

  $\mathcal{S}_{\delta}(\mu\alpha w\{[\alpha]\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v)/[\alpha]t\})$

  $\qquad = \mathcal{S}_{\delta}(w\{[\alpha]\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v)/[\alpha]t\})$

  $\qquad \subseteq \mathcal{S}_{\delta}(u)[\mathcal{S}_{\alpha}(w)/x] \cup \mathcal{S}_{\delta}(v)[\mathcal{S}_{\alpha}(w)/y] \cup \mathcal{S}_{\delta}(w)$

  $\qquad = \mathcal{S}_{\delta}(u)[\mathcal{S}_{[]}(\mu\alpha w)/x] \cup \mathcal{S}_{\delta}(v)[\mathcal{S}_{[]}(\mu\alpha w)/y] \cup \mathcal{S}_{\delta}(\mu\alpha w) = \mathcal{S}_{\delta}(r)$

$\square$

Lemma 3.4.7 *Given two $\lambda\mu^+$-term t, u and a context (a term with a hole) $C[\bullet]$, if $\mathcal{S}_{[]}(u) \subseteq \mathcal{S}_{[]}(t)$ and $\mathcal{S}_{\delta}(u) \subseteq \mathcal{S}_{\delta}(t)$ then $\mathcal{S}_{[]}(C[u]) \subseteq \mathcal{S}_{[]}(C[t])$ and $\mathcal{S}_{\delta}(C[u]) \subseteq \mathcal{S}_{\delta}(C[t])$ for any a free μ-variable δ of $C[t]$.*

Proof. By induction on the context $C[\bullet]$. $\square$

Proposition 3.4.8 *Given a $\lambda\mu^+$-term t, if t is μ-safe and $t \leadsto u$ then $\mathcal{S}_{[]}(u) \subseteq \mathcal{S}_{[]}(t)$ and $\mathcal{S}_{\delta}(u) \subseteq \mathcal{S}_{\delta}(t)$ for any a free μ-variable δ of t.*

Proof. By lemma 3.4.6 and lemma 3.4.7. $\square$

Lemma 3.4.9 *Given two $\lambda\mu^+$-terms u, v, if u and v are μ-safe then $u\{v/x\}$ is μ-safe.*

Proof. Let $\lambda y.t$ be a subterm of $u\{v/x\}$. Either $\lambda y.t$ is a subterm of v or y does not occur in v. Consequently, $y \notin \mathcal{S}_{\delta}(t)$ since v is μ-safe in the former case and since u is μ-safe in the latter case. $\square$

Lemma 3.4.10 *Given an instance $r \leadsto s$ of a rule of the $\lambda\mu^+$-calculus, if r is μ-safe then s is μ-safe.*

Proof. Again, we consider each rule of the $\lambda\mu^+$-calculus:

- $r = (\lambda x.u \; v)$ and $s = u\{v/x\}$. Apply lemma 3.4.9.

- $r = (\mu\alpha.u \; v)$ and $s = \mu\alpha.u\{[\alpha](w \; v)/[\alpha]w\}$. Let $\lambda y.t$ be a subterm of $\mu\alpha.u\{[\alpha](w \; v)/[\alpha]w\}$, either $\lambda y.t$ is a subterm of v or y does not occur in v. Consequently, $y \notin \mathcal{S}_{\delta}(t)$ since v is μ-safe in the former case and since u is μ-safe in the latter case.

- $r = [\beta]\mu\alpha.u$ and $s = u\{\beta/\alpha\}$. Let $\lambda y.t$ be a subterm of $u\{\beta/\alpha\}$ and let $\lambda y.v$ be the subterm of u such as $\lambda y.v = \lambda y.t\{\beta/\alpha\}$. Then $y \notin \mathcal{S}_{\delta}(t) = \mathcal{S}_{\delta}(v)$ and $y \notin \mathcal{S}_{\beta}(t) = \mathcal{S}_{\beta}(v) \cup \mathcal{S}_{\alpha}(v)$ since u is μ-safe.

- $r = \mu\alpha[\alpha]u$ and $s = u$ where α does not occur free in u. Then $s = u$ is μ-safe.

- $r = \textbf{let } x = u \textbf{ in } t$ and $s = t\{u/x\}$. Apply lemma 3.4.9.

- $r = \textbf{cases } (\textbf{inl } t) \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v$ and $s = u\{t/x\}$. Apply lemma 3.4.9.

- $r = \textbf{cases } \mu\alpha w \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v$

  and $s = \mu\alpha w\{[\alpha]\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v)/[\alpha]t\}$. Let $\lambda y.t$ be a subterm of $\mu\alpha w\{[\alpha]\textbf{cases } t \textbf{ of } (\textbf{inl } x) \mapsto u \mid (\textbf{inr } y) \mapsto v)/[\alpha]t\}$, either $\lambda y.t$ is a subterm of u or v or y does not occur in u, v. Consequently, $y \notin \mathcal{S}_\delta(t)$ since u, v are μ-safe in the former case and since w is μ-safe in the latter case.

$\square$

Theorem 3.4.11 *Given a $\lambda\mu^+$-term t, if t is μ-safe and $t \leadsto u$ then u is μ-safe.*

Proof. Let r be the redex of t which is reduced in $t \leadsto u$ and let r' be the contractum. Now, let us consider a subterm of u which has the form $\lambda y.s'$ and where δ is free μ-variable of s'. We have to prove that $y \notin \mathcal{S}_\delta(s')$. Three cases may occur: either r' and $\lambda y.s'$ do not overlap, or r' is a subterm of s', or $\lambda y.s'$ is a subterm of r'. The first case is trivial since $\lambda y.s'$ was already a subterm of t (which is μ-safe). In the second case, since t is μ-safe then r is μ-safe and $y \notin \mathcal{S}_\delta(r)$, by proposition 3.4.8, $\mathcal{S}_\delta(r') \subseteq \mathcal{S}_\delta(r)$ and thus $y \notin \mathcal{S}_\delta(r')$. In the last case, just apply lemma 3.4.10. $\square$

3.4.1 Typing μ-safe $\lambda\mu^+$-terms in $\overline{\text{CND}}^r_\vee$

By construction, constructive proofs of $\overline{\text{CND}}_\vee$ and μ-safe $\lambda\mu^+$-terms are related by the following theorem (and its corollary):

Theorem 3.4.12 *Given the derivation of a type judgement $t : \Gamma_1^{x_1}, \dots, \Gamma_n^{x_n} \vdash \Delta_1^{\alpha_1}, \dots, \Delta_m^{\alpha_m}; A$ in $\overline{\text{CND}}_\vee$, if $x_i \in \mathcal{S}_{\alpha_j}(t)$ then there is a link between $\Gamma_i^{x_i}$ and $\Delta_j^{\alpha_j}$ and if $x_i \in \mathcal{S}_{[]}(t)$ then there is a link between $\Gamma_i^{x_i}$ and A.*

Proof. Rephrase the definition of $\overline{\text{CND}}$ in such a way that the name of the rightmost formula of each sequent is always $[]$. Then, check that we have two inductive definitions of the same relation. $\square$

Corollary 3.4.13 *Given a derivation of the type judgement $t : \Gamma \vdash \Delta$ in $\text{CND}_\vee$, if t is μ-safe then the derivation of $t : \Gamma \vdash \Delta$ belongs to $\overline{\text{CND}}^r_\vee$ (and $\Gamma \vdash \Delta$ is valid in DIS-logic). Conversely, given a proof of $\Gamma \vdash \Delta$ in $\overline{\text{CND}}^r_\vee$, the $\lambda\mu^+$-term extracted from the proof is μ-safe.*

Proof. Let us consider an occurrence of the introduction rule of implication and let $\lambda x.u$ be the corresponding subterm of t, where u is typable of type $\Gamma_1^{x_1}, \dots, \Gamma_n^{x_n}, A^x \vdash \Delta_1^{\alpha_1}, \dots, \Delta_m^{\alpha_m}; B$. Since t is μ-safe, for any α_j, $x \notin \mathcal{S}_{\alpha_j}(u)$ and then by the theorem, there is no link between A^x and any $\Delta_j^{\alpha_j}$, thus this occurrence of the introduction rule of implication is constructive. $\square$

4 Directions for extensions

We have defined a restriction of the $\lambda\mu^+$-calculus, which is stable under reduction and whose type system corresponds to DIS-logic. In this calculus, continuations are not first-class objects but the ability of context-switching remains. We did not consider tag-abstraction (i.e. first-class μ-contexts) in this paper. A forthcoming paper will be devoted to this issue: we need a new connector (i.e. a new type constructor), called subtraction, which is dual to implication to type μ-contexts. We will thus obtain a λ-calculus with first-class coroutines, whose type system corresponds to subtractive logic (which a conservative extension of DIS-logic [22, 5, 4]).

We have proved that DIS-logic is constructive. We conjecture that is it possible to define a set of reduction rules for the $\lambda\mu^+$-calculus in which a normal form is canonical (a normal form does not begin with a $\mu\alpha[\alpha]$), or in other words, the last rule of a normal proof of $\overline{\text{CND}}_\vee^r$ is an introduction rule and not a right-hand contraction.

This conjecture raises a new question since subtractive logic is conservative over DIS-logic: can we define a set of reduction rules for a calculus whose type system is subtractive logic and in which a typed normal form is canonical if its type contains no subtraction?

A   Appendix

A.1   Conservativity of $\text{CND}_\vee^i$ over NJ+DIS

In this appendix, we show that $\overline{\text{CND}}_\vee^i$ is conservative over DIS-logic (in the propositional, the first and the second order frameworks). Indeed, any derivation of a sequent in $\overline{\text{CND}}_\vee^i$ can be translated into a derivation which does not contain any introduction rule of implication, but which uses axioms valid in DIS-logic.

The tricky part of the proof consists in showing that the generalized introduction rule of implication *commutes* with any other rule. We will also show that the generalized introduction rule of implication does not raise any problem when it is applied directly to a sequent valid in DIS-logic.

Theorem A.1.1 *The system* $\overline{\text{CND}}_\vee^i$ *is conservative over* DIS-logic .

Proof. We denote $hyp(\Delta)$ the set of (occurrences of) hypothesis linked to at least one of (occurrences of) a conclusions of Δ and let us consider the following generalization of the constructive introduction rule of implication:

$$\frac{\Gamma \vdash \Delta}{\Gamma\backslash\{H\} \vdash \Delta\backslash S, H \Rightarrow S^\vee} \quad \text{where } H \notin hyp(\Delta\backslash S)$$

Notice that H does not need to occur in Γ, and each occurence of hypothesis of S does not need to occur (and possibly none does) in Δ.

The tricky part of the proof consists in showing that the generaized introduction rule of implication *commutes* with any other rule (see section A.3). We will also show that the generalized introduction rule of implication does not raise any problem when it is applied directly to a sequent valid in DIS-logic (see section A.2). □

A.2   Axioms

Proposition A.2.1 *In* $\overline{\text{CND}}^+$, *the set of sequents that belong to one of the three following collections:*

- $\Gamma, A \vdash \Delta, B$ where $A \vdash B$ is valid in DIS-logic, and there is at most one link which annotates this sequent, and this link binds A and B together.

- $\Gamma, Y \vdash \Delta$ where $Y \vdash \bot$ is valid in DIS-logic,

- $\Gamma \vdash \Delta, X$ where $\top \vdash X$ is valid in DIS-logic.

is closed under the generalized introduction rule of implication.

Proof. Let us consider the generalized introduction rule of implication for the three collections of sequents:

1. The upper sequent has the form $\Gamma, A \vdash \Delta, B$ where $A \vdash B$ is valid in DIS-logic, and the unique link which annotates this sequent binds A and B together.

   - First case, $H \neq A$ and $B \notin S$.

   $$\frac{\Gamma, A \vdash \Delta, B}{\Gamma \backslash \{H\}, A \vdash \Delta \backslash S, B, H \Rightarrow S^\vee}$$

   the lower sequent is indeed of the first form.

   - Second case, $H \neq A$ and H is discharged on $S \cup \{B\}$

   $$\frac{\Gamma, A \vdash \Delta, B}{\Gamma \backslash \{H\}, A \vdash \Delta \backslash S, H \Rightarrow (S^\vee \vee B)}$$

   the lower sequent is indeed of the third form since if $A \vdash B$ is valid in DIS-logic and $B \in S$ then $A \vdash H \Rightarrow (S^\vee \vee B)$ is also valid.

   - Third case, $H = A$ and A is discharged on $S \cup \{B\}$

   $$\frac{\Gamma, A \vdash \Delta, B}{\Gamma \vdash \Delta \backslash S, A \Rightarrow (S^\vee \vee B)}$$

   the lower sequent is indeed of the third form since in NJ, if $A \vdash B$ is valid in DIS-logic then $\top \vdash A \Rightarrow (S^\vee \vee B)$ is also valid.

   In the case $H = A$ and $B \notin S$, i.e. where A is discharged on another conclusion that B, the constructive constraint does not hold. Consequently this case has not to be considered.

2. The upper sequent has the form $\Gamma, Y \vdash \Delta$ where $Y \vdash \perp$ is valid in DIS-logic.

   - First case, $H \neq Y$ and $H \notin hyp(\Delta \backslash S)$

   $$\frac{\Gamma, Y \vdash \Delta}{\Gamma \backslash \{H\}, Y \vdash \Delta \backslash S, H \Rightarrow S^\vee}$$

   the lower sequent is still of the second form.

   - Second case, $H = Y$ and $Y \notin hyp(\Delta \backslash S)$

   $$\frac{\Gamma, Y \vdash \Delta}{\Gamma \vdash \Delta \backslash S, Y \Rightarrow S^\vee}$$

   Since $Y \vdash \perp$ is valid in DIS-logic, we infer that $Y \vdash S^\vee$ and thus $\top \vdash Y \Rightarrow S^\vee$ is also valid in DIS-logic, and the lower sequent is thus of the third form.

3. The upper sequent has the form $\Gamma \vdash \Delta, X$ where $\top \vdash X$ is valid in DIS-logic.

   - First case, $X \notin S$

   $$\frac{\Gamma \vdash \Delta, X}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, X, H \Rightarrow S^\vee}$$

   the lower sequent is still of the third form.

   - Second case, H is discharged on $S \cup \{X\}$

   $$\frac{\Gamma \vdash \Delta, X}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, H \Rightarrow (S^\vee \vee X)}$$

   Since $\top \vdash X$ is derivable in DIS-logic, we infer that $H \vdash S^\vee \vee X$ and thus $\top \vdash H \Rightarrow (S^\vee \vee X)$ are also valid in DIS-logic, and the lower sequent is thus still of the third form.

the closure under the rule that discharge a conclusion is obtained by duality. □

A.3   Rules

Left weakening rule

- First case, $H \neq A$:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta}{\Gamma, A \vdash^2 \Delta}}{\Gamma \backslash \{H\}, A \vdash^3 \Delta \backslash S, A \Rightarrow S^\vee}$$

  where $H \notin hyp_2(\Delta \backslash S)$ and thus $H \notin hyp_1(\Delta \backslash S)$

  Replace by:

$$\frac{\dfrac{\Gamma \vdash \Delta}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, A \Rightarrow S^\vee}}{\Gamma \backslash \{H\}, A \vdash \Delta \backslash S, A \Rightarrow S^\vee}$$

- Second case, $H = A$:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta}{\Gamma, A \vdash^2 \Delta}}{\Gamma \vdash^3 \Delta \backslash S, A \Rightarrow S^\vee}$$

  where $A \notin hyp_2(\Delta \backslash S)$ and thus $A \notin hyp_1(\Delta \backslash S)$

  Replace by

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta \backslash S, A \Rightarrow S^\vee}$$

Left contraction rule

- First case, $H = A^z$:

$$\frac{\dfrac{\Gamma, A^x, A^y \vdash^1 \Delta}{\Gamma, A^z \vdash^2 \Delta}}{\Gamma \vdash^3 \Delta \backslash S, A \Rightarrow S^\vee}$$

  where $A^z \notin hyp_2(\Delta \backslash S)$ and thus $A^x \notin hyp_1(\Delta \backslash S)$ and $A^y \notin hyp_1(\Delta \backslash \{B^S\})$

  Replace by:

$$\frac{\dfrac{\Gamma, A^x, A^y \vdash \Delta}{\Gamma, A^z \vdash \Delta \backslash S, A \Rightarrow S^\vee}}{\Gamma \vdash \Delta \backslash S, A \Rightarrow (A \Rightarrow S^\vee)}$$

  and then cut with the sequent $A \Rightarrow (A \Rightarrow S^\vee) \vdash A \Rightarrow S^\vee$ valid in intuitionistic logic.

- Second case, $H \neq A^z$:

$$\frac{\dfrac{\Gamma, A^x, A^y \vdash^1 \Delta}{\Gamma, A^z \vdash^2 \Delta}}{\Gamma \backslash \{H\}, A^z \vdash^3 \Delta \backslash S, H \Rightarrow S^\vee}$$

  where $H \notin hyp_2(\Delta \backslash S)$ and thus $H \notin hyp_1(\Delta \backslash S)$

  Replace by:

$$\frac{\dfrac{\Gamma, A^x, A^y, H \vdash \Delta}{\Gamma \backslash \{H\}, A^x, A^y \vdash \Delta \backslash S, H \Rightarrow S^\vee}}{\Gamma \backslash \{H\}, A^z \vdash \Delta \backslash S, H \Rightarrow S^\vee}$$

Right contraction rule

- First case, $B \notin S$:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta, B^\alpha, B^\beta}{\Gamma \vdash^2 \Delta, B^\gamma}}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow S^\vee, B^\gamma}$$

where $H \notin hyp_2(\Delta \backslash S, B^\gamma)$ and thus $H \notin hyp_1(\Delta \backslash S, B^\alpha, B^\beta)$

Replace by:

$$\frac{\dfrac{\Gamma \vdash \Delta, B, B}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, H \Rightarrow S^\vee, B, B}}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, H \Rightarrow S^\vee, B}$$

- Second case, H is discharged on $S \cup \{B\}$:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta, B^\alpha, B^\beta}{\Gamma \vdash^2 \Delta, B^\gamma}}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow (S^\vee \vee B)}$$

where $H \notin hyp_2(\Delta \backslash S, B^\gamma)$ and thus $H \notin hyp_1(\Delta \backslash S, B^\alpha, B^\beta)$

Replace by:

$$\frac{\Gamma \vdash \Delta, B, B}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, H \Rightarrow (S^\vee \vee B \vee B)}$$

and then cut with the sequent $H \Rightarrow (S^\vee \vee B \vee B) \vdash H \Rightarrow (S^\vee \vee B)$ valid in intuitionistic logic.

Right weakening rule

- First case, $B \notin S$:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta}{\Gamma \vdash^2 \Delta, B}}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow S^\vee, B}$$

where $H \notin hyp_2(\Delta \backslash S, B)$ and thus $H \notin hyp_1(\Delta \backslash S)$

Replace by:

$$\frac{\dfrac{\Gamma \vdash \Delta}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, H \Rightarrow S^\vee}}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, H \Rightarrow S^\vee, B}$$

- Second case, H is discharged on $S \cup \{B\}$:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta}{\Gamma \vdash^2 \Delta, B^\alpha}}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow (S^\vee \vee B)}$$

where $H \notin hyp_2(\Delta \backslash S, B^\alpha)$ and thus $H \notin hyp_1(\Delta \backslash S)$

Replace by:

$$\frac{\Gamma \vdash \Delta}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, H \Rightarrow S^\vee}$$

and then cut with the sequent $H \Rightarrow S^\vee \vdash H \Rightarrow (S^\vee \vee B)$ valid in intuitionistic logic.

Right elimination rule for the implication

- First case, $B \notin S$:

$$\frac{\dfrac{\Gamma' \vdash^1 \Delta', A \Rightarrow B \qquad \Gamma'' \vdash^4 \Delta'', A}{\Gamma', \Gamma'' \vdash^2 \Delta', \Delta'', B}}{(\Gamma', \Gamma'') \backslash \{H\} \vdash^3 (\Delta', \Delta'') \backslash S, B, H \Rightarrow S^\vee}$$

where $H \notin hyp_2(B, (\Delta', \Delta'') \backslash S)$ and thus, by posing $S' = S \cap \Gamma'$ and $S'' = S \cap \Gamma''$, we have $H \notin hyp_1(A \Rightarrow B, \Delta \backslash S')$ and $H \notin hyp_4(A, \Delta \backslash S')$

Replace by:

$$\frac{\dfrac{\Gamma' \vdash \Delta', A \Rightarrow B}{\Gamma' \backslash \{H\} \vdash \Delta' \backslash S', H \Rightarrow S'^\vee, A \Rightarrow B} \qquad \dfrac{\Gamma'' \vdash \Delta'', A}{\Gamma'' \backslash \{H\} \vdash \Delta'' \backslash S'', H \Rightarrow S''^\vee, A}}{\dfrac{(\Gamma', \Gamma'') \backslash \{H\} \vdash (\Delta', \Delta'') \backslash S, H \Rightarrow S'^\vee, H \Rightarrow S''^\vee, B}{(\Gamma', \Gamma'') \backslash \{H\} \vdash (\Delta', \Delta'') \backslash S, (H \Rightarrow S'^\vee) \vee (H \Rightarrow S''^\vee), B}}$$

and then cut with the sequent $(H \Rightarrow S'^\vee) \vee (H \Rightarrow S''^\vee) \vdash H \Rightarrow (S'^\vee \vee S''^\vee)$ valid in intuitionistic logic.

- Second case, H is discharged on $S \cup \{B\}$::

$$\frac{\dfrac{\Gamma' \vdash^1 \Delta', A \Rightarrow B \qquad \Gamma'' \vdash^4 \Delta'', A}{\Gamma', \Gamma'' \vdash^2 \Delta', \Delta'', B}}{(\Gamma', \Gamma'') \backslash \{H\} \vdash^3 (\Delta', \Delta'') \backslash S, H \Rightarrow (S^\vee \vee B)}$$

where $H \notin hyp_2((\Delta', \Delta'') \backslash S)$ and thus, by posing $S' = S \cap \Gamma'$ and $S'' = S \cap \Gamma''$, there is $H \notin hyp_1(\Delta \backslash S')$ and $H \notin hyp_4(\Delta \backslash S')$.

Replace by:

$$\frac{\dfrac{\Gamma' \vdash \Delta', A \Rightarrow B}{\Gamma' \backslash \{H\} \vdash \Delta' \backslash S', H \Rightarrow (S'^\vee \vee (A \Rightarrow B))} \qquad \dfrac{\Gamma'' \vdash \Delta'', A}{\Delta'' \backslash S', H \Rightarrow (S''^\vee \vee A)}}{(\Gamma', \Gamma'') \backslash \{H\} \vdash (\Delta', \Delta'') \backslash S, (H \Rightarrow (S'^\vee \vee (A \Rightarrow B))) \wedge (H \Rightarrow (S''^\vee \vee A))}$$

and then cut with the sequent $(H \Rightarrow (S'^\vee \vee (A \Rightarrow B))) \wedge (H \Rightarrow (S''^\vee \vee A)) \vdash H \Rightarrow (S^\vee \vee B)$ valid in intuitionistic logic.

Left introduction rule of disjunction

- First case, $H \neq A \vee B$:

$$\frac{\dfrac{\Gamma', A \vdash^1 \Delta' \qquad \Gamma'', B \vdash^4 \Delta''}{\Gamma', \Gamma'', A \vee B \vdash^2 \Delta', \Delta''}}{(\Gamma', \Gamma'') \backslash \{H\}, A \vee B \vdash^3 (\Delta', \Delta'') \backslash S, H \Rightarrow S^\vee}$$

where $H \notin hyp_2((\Delta', \Delta'') \backslash S)$ and thus, by posing $S' = S \cap \Gamma'$ and $S'' = S \cap \Gamma''$, we have $H \notin hyp_1(\Delta \backslash S')$ and $H \notin hyp_4(\Delta \backslash S')$

Replace by:

$$\frac{\dfrac{\Gamma', A \vdash \Delta'}{\Gamma' \backslash \{H\}, A \vdash \Delta' \backslash S', H \Rightarrow S'^\vee} \qquad \dfrac{\Gamma'', B \vdash \Delta''}{\Gamma'' \backslash \{H\}, B \vdash \Delta'', H \Rightarrow S''^\vee}}{\dfrac{(\Gamma', \Gamma'') \backslash \{H\}, A \vee B \vdash (\Delta', \Delta'') \backslash S, H \Rightarrow S'^\vee, H \Rightarrow S''^\vee}{(\Gamma', \Gamma'') \backslash \{H\}, A \vee B \vdash (\Delta', \Delta'') \backslash S, (H \Rightarrow S'^\vee) \vee (H \Rightarrow S''^\vee)}}$$

and then cut with the sequent $(H \Rightarrow S'^\vee) \vee (H \Rightarrow S''^\vee) \vdash H \Rightarrow (S'^\vee \vee S''^\vee)$ valid in intuitionistic logic.

- Second case, $H = A \vee B$:

$$\frac{\dfrac{\Gamma', A \vdash^1 \Delta' \qquad \Gamma'', B \vdash^4 \Delta''}{\Gamma', \Gamma'', A \vee B \vdash^2 \Delta', \Delta''}}{\Gamma', \Gamma'' \vdash^3 (\Delta', \Delta'') \backslash S, A \vee B \Rightarrow S^\vee}$$

where $A \vee B \notin hyp_2((\Delta', \Delta'') \backslash S)$ and thus, by posing $S' = S \cap \Gamma'$ and $S'' = S \cap \Gamma''$, we have $A \notin hyp_1(\Delta \backslash S')$ and $B \notin hyp_4(\Delta \backslash S')$.

Replace by:

$$\frac{\dfrac{\Gamma', A \vdash \Delta'}{\Gamma' \backslash \{H\} \vdash \Delta' \backslash S', A \Rightarrow S'^\vee} \qquad \dfrac{\Gamma'', B \vdash \Delta''}{\Delta'' \backslash S', B \Rightarrow S''^\vee}}{(\Gamma', \Gamma'') \backslash \{H\} \vdash (\Delta', \Delta'') \backslash S, (A \Rightarrow S'^\vee) \wedge (B \Rightarrow S''^\vee)}$$

and then cut with the sequent $(A \Rightarrow S'^\vee) \wedge (B \Rightarrow S''^\vee) \vdash (A \vee B) \Rightarrow (S'^\vee \vee S''^\vee)$ valid in intuitionistic logic.

Left elimination rule of disjunction   We consider only the case of the first *injection*, the second may be treated in a similar way.

- First case, $H \neq A$:

$$\frac{\dfrac{\Gamma, A \vee B \vdash^1 \Delta}{\Gamma, A \vdash^2 \Delta}}{\Gamma \backslash \{H\}, A \vdash^3 \Delta \backslash S, H \Rightarrow S^\vee}$$

where $H \notin hyp_2(\Delta \backslash S)$ and thus $H \notin hyp_1(\Delta \backslash S)$

Replace by:

$$\frac{\dfrac{\Gamma, A \vee B \vdash \Delta}{\Gamma \backslash \{H\}, A \vee B \vdash \Delta \backslash S, H \Rightarrow S^\vee}}{\Gamma \backslash \{H\}, A \vdash \Delta \backslash S, H \Rightarrow S^\vee}$$

- Second case, $H = A$:

$$\frac{\dfrac{\Gamma, A \vee B \vdash^1 \Delta}{\Gamma, A \vdash^2 \Delta}}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, A \Rightarrow S^\vee}$$

where $H \notin hyp_2(\Delta \backslash S)$ and thus $H \notin hyp_1(\Delta \backslash S)$ and $A \notin hyp_4(\Delta \backslash S)$

Replace by:

$$\frac{\Gamma, A \vee B \vdash \Delta}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, (A \vee B) \Rightarrow S^\vee}$$

and then cut with the sequent $(A \vee B) \Rightarrow S^\vee \vdash A \Rightarrow S^\vee$ valid in intuitionistic logic.

Cut rule

$$\frac{\dfrac{\Gamma' \vdash^1 A, \Delta' \qquad \Gamma'', A \vdash^4 \Delta''}{\Gamma', \Gamma'' \vdash^2 \Delta', \Delta''}}{(\Gamma', \Gamma'') \backslash \{H\} \vdash^3 (\Delta', \Delta'') \backslash S, H \Rightarrow S^\vee}$$

where $H \notin hyp_2((\Delta', \Delta'') \backslash S)$ and thus, by posing $S' = S \cap \Gamma'$ and $S'' = S \cap \Gamma''$:

- First case, $H \notin \Gamma'$

  Replace by:

$$\frac{\dfrac{\Gamma' \vdash \Delta', A}{\Gamma' \vdash \Delta' \backslash S', H \Rightarrow S'^\vee, A} \qquad \dfrac{\Gamma'', A \vdash \Delta''}{\Gamma'' \backslash \{H\}, A \vdash \Delta'' \backslash S', H \Rightarrow S''^\vee}}{\dfrac{(\Gamma', \Gamma'') \backslash \{H\} \vdash (\Delta', \Delta'') \backslash S, H \Rightarrow S'^\vee, H \Rightarrow S''^\vee}{(\Gamma', \Gamma'') \backslash \{H\} \vdash (\Delta', \Delta'') \backslash S, (H \Rightarrow S'^\vee) \vee (H \Rightarrow S''^\vee)}}$$

  then cut with the sequent $(H \Rightarrow S'^\vee) \vee (H \Rightarrow S''^\vee) \vdash H \Rightarrow (S'^\vee \vee S''^\vee)$ valid in intuitionistic logic.

- Second case, $H \notin \Gamma''$ and $H \notin hyp_1(A)$ since $H \notin hyp_1(A, \Delta' \backslash S')$

  Replace by:

$$\frac{\dfrac{\Gamma' \vdash \Delta', A}{\Gamma' \backslash \{H\} \vdash \Delta' \backslash S', H \Rightarrow S'^\vee, A} \qquad \dfrac{\Gamma'', A \vdash \Delta''}{\Gamma'', A \vdash \Delta'' \backslash S', H \Rightarrow S''^\vee}}{\dfrac{(\Gamma', \Gamma'') \backslash \{H\} \vdash (\Delta', \Delta'') \backslash S, H \Rightarrow S'^\vee, H \Rightarrow S''^\vee}{(\Gamma', \Gamma'') \backslash \{H\} \vdash (\Delta', \Delta'') \backslash S, (H \Rightarrow S'^\vee) \vee (H \Rightarrow S''^\vee)}}$$

  then cut with the sequent $(H \Rightarrow S'^\vee) \vee (H \Rightarrow S''^\vee) \vdash H \Rightarrow (S'^\vee \vee S''^\vee)$ valid in intuitionistic logic.

- Third case, $H \in \Gamma'$ and $H \in hyp_1(A)$ and since $H \notin hyp_1(\Delta'' \backslash S'')$ we have $A \notin hyp_1(\Delta'' \backslash S')$.

  Replace by:

$$\frac{\dfrac{\Gamma' \vdash \Delta', A}{\Gamma' \backslash \{H\} \vdash \Delta' \backslash S', H \Rightarrow (S'^\vee \vee A)} \qquad \dfrac{\Gamma'', A \vdash \Delta''}{\Gamma'' \vdash \Delta' \backslash S', A \Rightarrow S''^\vee}}{(\Gamma', \Gamma'') \backslash \{H\} \vdash (\Delta', \Delta'') \backslash S, (H \Rightarrow (S'^\vee \vee A)) \wedge (A \Rightarrow S''^\vee)}$$

  then cut with the sequent $(H \Rightarrow (S'^\vee \vee A)) \wedge (A \Rightarrow S''^\vee) \vdash H \Rightarrow (S'^\vee \vee S''^\vee)$ valid in intuitionistic logic.

A.4 Quantifiers

We only deal with the first order quantifier, the case of $\forall^2$ is similar.

Right introduction rule for $\forall$ (where x does not occur in Γ, Δ)

- First case, $\forall x A \notin S$:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta, A}{\Gamma \vdash^2 \Delta, \forall x A}}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow S^\vee, \forall x A}$$

  where $H \notin hyp_2(\Delta \backslash S, \forall x A)$ and thus $H \notin hyp_1(\Delta \backslash S, A)$

  Replace by:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta, A}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow S^\vee, A}}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow S^\vee, \forall x A}$$

21

- Second case, H is discharged on $S \cup \{\forall x A\}$:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta, A}{\Gamma \vdash^2 \Delta, \forall x A}}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow (S^\vee \vee \forall x A)}$$

where $H \notin hyp_2(\Delta \backslash S)$ and thus $H \notin hyp_1(\Delta \backslash S)$ and $A \notin hyp_4(\Delta \backslash S)$

Replace by:

$$\frac{\dfrac{\Gamma \vdash \Delta, A}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, H \Rightarrow (S^\vee \vee A)}}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, \forall x(H \Rightarrow (S^\vee \vee A))}$$

and then cut with the sequent $\forall x(H \Rightarrow (S^\vee \vee A)) \vdash H \Rightarrow (S^\vee \vee \forall x A)$ valid in DIS-logic since x does not occur in $H, S^\vee$. Notice that DIS) is actually needed.

Right elimination rule for $\forall$

- First case, $A \notin S$:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta, \forall x A}{\Gamma \vdash^2 \Delta, A[t/x]}}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow S^\vee, A}$$

where $H \notin hyp_2(A[t/x], \Delta \backslash S)$ and thus $H \notin hyp_1(\forall x A, \Delta \backslash S)$

Replace by:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta, \forall x A}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow S^\vee, \forall x A}}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow S^\vee, A[t/x]}$$

- Second case, H is discharged on $S \cup \{\forall x A\}$:

$$\frac{\dfrac{\Gamma \vdash^1 \Delta, \forall x A}{\Gamma \vdash^2 \Delta, A[t/x]}}{\Gamma \backslash \{H\} \vdash^3 \Delta \backslash S, H \Rightarrow (S^\vee \vee A[t/x])}$$

where $H \notin hyp_2(\Delta \backslash S)$ and thus $H \notin hyp_1(\Delta \backslash S)$ and $A \notin hyp_4(\Delta \backslash S)$

Replace by:

$$\frac{\Gamma \vdash \Delta, \forall x A}{\Gamma \backslash \{H\} \vdash \Delta \backslash S, H \Rightarrow (S^\vee \vee A)}$$

then cut with the sequent $H \Rightarrow (S^\vee \vee \forall x A) \vdash H \Rightarrow (S^\vee \vee A[t/x])$ derivable NJ.

References

[1] F. Barbanera and S. Berardi. Extracting constructive content from classical logic via control-like reductions. volume 662 of *LNCS*, pages 47–59. Springer-Verlag, 1994.

[2] E. C. Cooper and J. G. Morrisett. Adding threads to standard ML. Report CMU-CS-90-186, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 1990.

[3] T. Crolard. A confluent lambda-calculus with a catch/throw mechanism. Submitted to the *Journal of Functional Programming*. (ftp://sweet-smoke.ufr-info-p7.jussieu.fr/crolard/jfp.ps).

[4] T. Crolard. From bicartesian closed categories with coexponents towards subtractive logic. Submitted to *Theoretical Computer Science*. (ftp://sweet-smoke.ufr-info-p7.jussieu.fr/crolard/tcs.ps).

[5] T. Crolard. Extension de l'isomorphisme de Curry-Howard au traitement des exceptions (application d'une étude de la dualité en logique intuitionniste). Thèse de Doctorat. Université Paris 7, 1996. (ftp://sweet-smoke.ufr-info-p7.jussieu.fr/crolard/these.ps).

[6] P. de Groote. A simple calculus of exception handling. In *Second International Conference on Typed Lambda Calculi and Applications*, LNCS, pages 201–215, Edinburgh, United Kingdom, 1995.

[7] A. G. Dragalin. Mathematical intuitionism–introduction to proof theory. In *Translations of Mathematical Monographs*, volume 67 of *American Matematical Society*. Providence, Rhode Island, 1988.

[8] R. Dyckhoff. Contraction-free sequent calculi for intuitionistic logic. *The Journal of Symbolic Logic*, 57(3):795–807, 1992.

[9] D. P. Friedman, C. T. Haynes, and M. Wand. Continuations and coroutines: An exercise in metaprogramming. In *Proc. 1984 ACM Symposium on Lisp and Functional Programming*, pages 293–298, August 1984.

[10] T. G. Griffin. A formulæ-as-type notion of control. In *Conference Record of the Seventeenth Annual ACM Symposium on Principles of Programming Langages*, pages 47–58, 1990.

[11] Y. Kameyama. A new formulation of the catch/throw mechanism. In T. Ida, A. Ohori, and M. Takeichi, editors, *Second Fuji International Workshop on Functional and Logic Programming*, Word Scientific, pages 106–122, 1997.

[12] Y. Kameyama and M. Sato. A classical catch/throw calculus with tag abstraction and its strong normalizability. In X. Lin, editor, *Proc. the 4th Australasian Theory Symposium*, volume 20-3 of *Australian Computer Science Communications*, pages 183–197. Springer-Verlag, 1998.

[13] J.-L. Krivine. Classical logic, storage operators and second order λ-calculus. *Ann. of Pure and Appl. Logic*, 68:53–78, 1994.

[14] C. R. Murthy. Classical proofs as programs: How, when, and why. Technical Report 91-1215, Cornell University, Department of Computer Science, 1991.

[15] H. Nakano. A constructive logic behind the catch and throw mechanism. *Annals of Pure and Applied Logic*, 69(3):269–301, 1994.

[16] H. Nakano. The non-deterministic catch and throw mechanism and its subject reduction property. In *Logic, Language and Computation*, volume 592 of *LNCS*, pages 61–72. Springer-Verlag, 1994.

[17] H. Nakano. *The Logical Structures of the Catch and Throw Mechanism*. PhD thesis, The University of Tokyo, 1995.

[18] M. Parigot. $\lambda\mu$-calculus: an algorithmic interpretation of classical natural deduction. In *Proc. Logic Prog. and Autom. Reasoning*, volume 624 of *LNCS*, pages 190–201, 1992.

[19] M. Parigot. Classical proofs as programs. In *Computationnal logic and theory*, volume 713 of *LNCS*, pages 263–276. Springer-Verlag, 1993.

[20] M. Parigot. Strong normalisation for second order classical natural deduction. In *Proceedings of the eighth annual IEEE symposium on logic in computer science*, 1993.

[21] N. Ramsey. Concurrent programming in ML. Technical Report CS-TR-262-90, Department of Computer Science, Princeton University, Princeton, NJ, 1990.

[22] C. Rauszer. An algebraic and Kripke-style approach to a certain extension of intuitionistic logic. In *Dissertationes Mathematicae*, volume 167. Institut Mathématique de l'Académie Polonaise des Sciences, 1980.

[23] N. J. Rehof and M. H. Sørensen. The λ_Δ-calculus. In *Theoritical Aspects of Computer Software*, volume 542 of *LNCS*, pages 516–542. Springer-Verlag, 1994.

[24] J. H. Reppy. Asynchronous signals is standard ML. Technical Report TR90-1144, Cornell University, Computer Science Department, August 1990.

[25] J. H. Reppy. First-class synchronous operations. *Lecture Notes in Computer Science*, 907:235–252, 1995.

[26] M. Sato. Intuitionistic and classical natural deduction systems with the Catch and the Throw rules. *Theoretical Computer Science*, 175(1):75–92, 1997.

[27] M. E. Szabo. *Gentzen Collected work*. North-Holland, Amsterdam, 1969.

[28] M. Wand. Continuation-based multiprocessing. In J. Allen, editor, *Conference Record of the 1980 LISP Conference*, pages 19–28, Palo Alto, CA, 1980. The Lisp Company. Republished by ACM.