

# The Russell-Prawitz embedding and the atomization of universal instantiation

José Espírito Santo  
Centro de Matemática  
Universidade do Minho  
4710-057 Braga  
Portugal  
jes@math.uminho.pt

Gilda Ferreira  
DCeT, Universidade Aberta, 1269-001 Lisboa, Portugal  
CMAFcIO, Faculdade de Ciências da Universidade de Lisboa,  
1749-016 Lisboa, Portugal  
gmferreira@fc.ul.pt

June 9, 2020

## Abstract

Given the recent interest in the fragment of system  $\mathbf{F}$  where universal instantiation is restricted to atomic formulas, a fragment nowadays named system  $\mathbf{F}_{\text{at}}$ , we study directly in system  $\mathbf{F}$  new conversions whose purpose is to enforce that restriction. We show some benefits of these new atomization conversions: (1) They help achieving strict simulation of proof reduction by means of the Russell-Prawitz embedding of  $\mathbf{IPC}$  into system  $\mathbf{F}$ ; (2) They are not stronger than a certain “dinaturality” conversion known to generate a consistent equality of proofs; (3) They provide the bridge between the Russell-Prawitz embedding and another translation, due to the authors, of  $\mathbf{IPC}$  directly into system  $\mathbf{F}_{\text{at}}$ ; (4) They give means for explaining why the Russell-Prawitz translation achieves strict simulation whereas the translation into  $\mathbf{F}_{\text{at}}$  does not.

**Keywords:** Intuitionistic propositional calculus, system  $\mathbf{F}$ , predicative polymorphism, Russell-Prawitz translation, proof reduction.

## 1 Introduction

The Russell-Prawitz translation of the intuitionistic propositional calculus  $\mathbf{IPC}$  into second-order intuitionistic propositional calculus  $\mathbf{NI}^2$ , the latter based on the language only containing implication, conjunction and the second-order universal quantifier,

rests on the following encoding of disjunction and absurdity  $A \vee B := \forall X.((A \supset X) \wedge (B \supset X)) \supset X$  and  $\perp := \forall X.X$ . This encoding is due to Prawitz but its idea goes back to Russell [10]. Under the Curry-Howard correspondence, the target of the translation can be taken to be Girard’s polymorphic system  $\mathbf{F}$  [7].

At the level of proofs, while the translation of the introduction rule for disjunction is straightforward, there are several alternatives for the translation of the elimination rules for the encoded connectives. The most direct one makes full use of the elimination rule for the second order quantifier. For instance, given in  $\mathbf{F}$  a “foreign” formula  $C$  and proofs of  $A \supset C$  and  $B \supset C$ , it is immediate to obtain a proof of  $C$  from a proof of  $A \vee B$  as defined above, starting by an instantiation of the quantifier to the formula  $C$ . This idea is implicit in [10] - we will confirm this later on in this paper. Following [1, 6, 11], we are calling Russell-Prawitz translation the translation of  $\mathbf{IPC}$  into system  $\mathbf{F}$  based on this translations of proofs.

There are alternative translations of  $\mathbf{IPC}$  proofs, still employing the Russell-Prawitz translation of formulas, which make a restricted use of the elimination rule for the second order quantifier, only requiring instantiation by atomic formulas. One such translation is based on the idea of “instantiation overflow” [4, 5] - the observation that full instantiation of the quantifiers in formulas of the form  $A \vee B$  or  $\perp$  as above is derivable in system  $\mathbf{F}_{\text{at}}$  - the restriction of system  $\mathbf{F}$  to atomic universal instantiations. Another translation of  $\mathbf{IPC}$  into  $\mathbf{F}_{\text{at}}$ , always with the same translation of formulas, was proposed recently by the authors [3] and is based on the observation that the elimination rules for the defined connectives are derivable in  $\mathbf{F}_{\text{at}}$ .

There are several reasons to study embeddings of  $\mathbf{IPC}$  into  $\mathbf{F}_{\text{at}}$ , the foremost being that  $\mathbf{F}_{\text{at}}$  is a predicative fragment of  $\mathbf{F}$ . Another reason has to do with preservation of proof identities generated in  $\mathbf{IPC}$  by commuting conversions or  $\eta$ -reductions: the various embeddings into  $\mathbf{F}_{\text{at}}$  achieve that preservation [5, 6, 3], while the Russell-Prawitz translation into  $\mathbf{F}$  does not [7, 12, 5, 6, 11]. This seems an indication that other conversion principles are missing in  $\mathbf{F}$ , besides the  $\beta\eta$  ones. Indeed, a general commuting principle, expressing “naturality” in the categorial semantics of  $\mathbf{F}$ , was suggested in [11], with good results for the problem of preservation of identity of proofs.

Given the interest in system  $\mathbf{F}_{\text{at}}$ , we study in system  $\mathbf{F}$  other conversions whose purpose is to enforce the restriction to atomic universal instantiation, with the goal of shedding light, not only on the problem of preservation of proof identity, but also on the existence of alternative embeddings of  $\mathbf{IPC}$  into  $\mathbf{F}$  and  $\mathbf{F}_{\text{at}}$ . We show that, when  $\mathbf{F}$  is equipped with these *atomization conversions*, the Russell-Prawitz translation achieves a strict simulation of proof reduction. Moreover, those conversions connect the Russell-Prawitz translation into system  $\mathbf{F}$  and the translation into system  $\mathbf{F}_{\text{at}}$  introduced by the authors. First, it is easy to establish a strong relation between the two translations at the level of proofs: given an  $\mathbf{IPC}$  proof, its translation into  $\mathbf{F}_{\text{at}}$  is the normal form of its translation into  $\mathbf{F}$  w.r.t. the atomization conversions. Second, a more laborious connection at the level of proof reduction is worked out, providing a comprehensive, detailed and clear picture of the problem of preservation of proof identity/reduction: indeed, as discussed in the final section of this paper, the key to the stronger preservation of proof *reduction* is the timing of atomization.

Of course, one has to be sure that adding those atomization conversions to system  $\mathbf{F}$  does not collapse proof identity. A similar problem was faced in [11], where a

“naturality” conversion was added to system  $\mathbf{F}$ . In that paper the following argument of consistency is outlined: the equality generated by adding the “naturality” conversions is contained in the equality generated by adding a stronger “dinaturality” conversion, and the latter equality is known to have models. Here we follow the same strategy to show with considerable detail that adding atomization conversions to system  $\mathbf{F}$  will not entail that any two terms are inter-convertible.

**Plan of the paper.** Section 2 recalls  $\mathbf{IPC}$  and systems  $\mathbf{F}$  and  $\mathbf{F}_{\text{at}}$ . Section 3 recalls the Russell-Prawitz translation, recasting it as a translation between typed  $\lambda$ -calculi. Section 4 introduces atomization conversions, relates them to other commuting conversions in system  $\mathbf{F}$ , and proves strict simulation by the Russell-Prawitz translation. Section 5 considers the Russell-Prawitz translation together with the embedding into  $\mathbf{F}_{\text{at}}$  due to the authors, relating them at the levels of proofs and proof reduction, through the atomization conversions. Section 6 rounds up the paper with a discussion.

## 2 Background

We present the systems we will use in the paper ( $\mathbf{IPC}$ ,  $\mathbf{F}$  and  $\mathbf{F}_{\text{at}}$ ).

### System $\mathbf{IPC}$

Throughout this work the interpreted system is the Intuitionistic Propositional Calculus ( $\mathbf{IPC}$ ), which we now recall.

The types/formulas in  $\mathbf{IPC}$  are given by

$$A, B, C ::= X \mid \perp \mid A \supset B \mid A \wedge B \mid A \vee B$$

We define  $\neg A := A \supset \perp$ .

The proof terms  $M, N, P, Q$  are inductively generated as follows:

$$\begin{array}{ll} M ::= & x \quad (\text{assumption}) \\ & \mid \lambda x^A. M \mid MN \quad (\text{implication}) \\ & \mid \langle M, N \rangle \mid M1 \mid M2 \quad (\text{conjunction}) \\ & \mid \text{in}_1(M, A, B) \mid \text{in}_2(N, A, B) \mid \text{case}(M, x^A.P, y^B.Q, C) \quad (\text{disjunction}) \\ & \mid \text{abort}(M, A) \quad (\text{absurdity}) \end{array}$$

We work modulo  $\alpha$ -equivalence, in particular we assume the name of the bound variables is always appropriately chosen.

Sometimes, when clear from the context or not relevant, the type annotations in the proof terms will be omitted. This applies to type annotations in binders, or for the last type parameter in  $\text{case}(M, x^A.P, y^B.Q, C)$  and  $\text{abort}(M, A)$ <sup>1</sup>. When possible and convenient, we write  $\langle P_1, P_2 \rangle$  as  $\langle P_i \rangle_{i=1,2}$ .

The typing/inference rules are in Fig. 1. A *sequent* is an expression  $\Gamma \vdash M : A$ . An *environment*  $\Gamma$  is a set of *declarations*  $x : A$  such that each variable is declared at

<sup>1</sup>Of course, one can define a version of proof terms for  $\mathbf{IPC}$  without the last type parameter in  $\text{case}(M, x^A.P, y^B.Q, C)$  and  $\text{abort}(M, A)$ . But, as in [3], that last type parameter makes it possible to define proof translations directly on proof terms. This happened in *op. cit.* with a translation into  $\mathbf{F}_{\text{at}}$ , and will happen in this paper with the Russell-Prawitz translation into  $\mathbf{F}$ .

Figure 1: Typing/inference rules of IPC

$$\begin{array}{c}
\overline{\Gamma, x : A \vdash x : A} \text{ Ass} \\
\\
\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x^A. M : A \supset B} \supset I \quad \frac{\Gamma \vdash M : A \supset B \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B} \supset E \\
\\
\frac{\Gamma \vdash M : A \quad \Gamma \vdash N : B}{\Gamma \vdash \langle M, N \rangle : A \wedge B} \wedge I \quad \frac{\Gamma \vdash M : A \wedge B}{\Gamma \vdash M1 : A} \wedge E1 \quad \frac{\Gamma \vdash M : A \wedge B}{\Gamma \vdash M2 : B} \wedge E2 \\
\\
\frac{\Gamma \vdash M : A}{\Gamma \vdash \text{in}_1(M, A, B) : A \vee B} \vee I1 \quad \frac{\Gamma \vdash N : B}{\Gamma \vdash \text{in}_2(N, A, B) : A \vee B} \vee I2 \\
\\
\frac{\Gamma \vdash M : A \vee B \quad \Gamma, x : A \vdash P : C \quad \Gamma, y : B \vdash Q : C}{\Gamma \vdash \text{case}(M, x^A.P, y^B.Q, C) : C} \vee E \\
\\
\frac{\Gamma \vdash M : \perp}{\Gamma \vdash \text{abort}(M, A) : A} \perp E
\end{array}$$

most one time in  $\Gamma$ . Given  $\Gamma$  and  $A$ ,  $M$  has type  $A$  in  $\Gamma$  if  $\Gamma \vdash M : A$  is derivable; given  $\Gamma$ ,  $M$  is *typable* in  $\Gamma$  if, for some  $A$ ,  $M$  has type  $A$  in  $\Gamma$ ; and  $M$  is *typable* if  $M$  is typable in some  $\Gamma$ .

For the purpose of discussing some reduction rules and defining the translation of proof terms, it is convenient to arrange the syntax of the system in a different way:

$$\begin{array}{lll}
\text{(Terms)} & M & ::= V \mid \mathcal{E}[M] \\
\text{(Values)} & V & ::= x \mid \lambda x. M \mid \langle M, N \rangle \mid \text{in}_1(M, A, B) \mid \text{in}_2(N, A, B) \\
\text{(Elim. contexts)} & \mathcal{E} & ::= [-]N \mid [-]1 \mid [-]2 \\
& & \mid \text{case}([-], x.P, y.Q, C) \mid \text{abort}([-], A)
\end{array}$$

A *value*  $V$  ranges over terms representing assumptions or introduction inferences.  $\mathcal{E}$  stands for an *elimination context*, which is a term representing an elimination inference, but with a “hole” in the position of the main premiss.  $\mathcal{E}[M]$  denotes the term resulting from filling the hole of  $\mathcal{E}$  with  $M$ .

In Fig. 2 one finds the typing rules for elimination contexts. In a sequent  $\Gamma \mid A \vdash \mathcal{E} : B$ , the type  $A$  is the type of the hole of  $\mathcal{E}$  and  $B$  is the type of the term obtained by filling the hole of  $\mathcal{E}$  with a term of type  $A$ . If the sequent  $\Gamma \mid A \vdash \mathcal{E} : B$  is derivable, we say  $\mathcal{E}$  has type  $B$  and hole of type  $A$  in  $\Gamma$ .

The reduction rules are given in Fig. 3. We let  $\beta := \beta_{\supset} \cup \beta_{\wedge} \cup \beta_{\vee}$  and similarly for  $\eta$ ; and we let  $\pi := \pi_{\supset} \cup \pi_{\wedge} \cup \pi_{\vee} \cup \pi_{\perp}$  and similarly for  $\varpi$ .

Given a reduction rule  $R$  of **IPC**, we employ the usual notations concerning reduction relations generated by  $R$ : the compatible closure<sup>2</sup> of  $R$  is denoted  $\rightarrow_R$ ; and  $\rightarrow_R^+$ ,

<sup>2</sup>A relation  $R$  on the proof terms is *compatible* if it is compatible with each proof-term constructor.

Figure 2: Typing rules for elimination contexts

$$\begin{array}{c}
\frac{}{\Gamma \vdash \perp \vdash \text{abort}([\_], A) : A} \quad \frac{}{\Gamma \vdash A_1 \wedge A_2 \vdash [\_]i : A_i} \quad (i = 1, 2) \\
\\
\frac{\Gamma \vdash N : A}{\Gamma \vdash A \supset B \vdash [\_]N : B} \quad \frac{\Gamma, x : A \vdash P : C \quad \Gamma, y : B \vdash Q : C}{\Gamma \vdash A \vee B \vdash \text{case}([\_], x.P, y.Q, C) : C} \\
\\
\frac{\Gamma \vdash M : A \quad \Gamma \vdash A \vdash \mathcal{E} : B}{\Gamma \vdash \mathcal{E}[M] : B}
\end{array}$$

$\rightarrow_R^*$ ,  $=_R$  denote respectively the transitive closure, the reflexive-transitive closure, and the reflexive-symmetric-transitive closure of  $\rightarrow_R$ . If  $R = R_1 \cup R_2$ , then we may omit “ $\cup$ ” in our notation and write  $\rightarrow_{R_1 R_2}$ , etc. The same notations apply to systems **F** and **F<sub>at</sub>** below.

For every reduction rule  $R$  of **IPC**,  $\rightarrow_R$  has the *subject reduction* property, that is: if  $M \rightarrow_R N$  and  $M$  has type  $A$  in  $\Gamma$ , then  $N$  has type  $A$  in  $\Gamma$ .

Notice  $\pi$  is contained in the following reduction rule:

$$\mathcal{E}[\text{case}(M, x^A.P, y^B.Q, C)] \rightarrow \text{case}(M, x^A.\mathcal{E}[P], y^B.\mathcal{E}[Q], D) \quad (1)$$

But the rules are not equivalent, as witnessed by the fact that the latter rule generates a reduction relation  $\rightarrow$  that does not enjoy subject reduction. This is caused by the fact that types  $C$  and  $D$  are unconstrained in (1), and so the connections that the various  $\pi$ -rules establish between the types  $C$  and  $D$  are not imposed in (1). For instance, in rule  $\pi_\supset$ ,  $C$  is an implication  $E \supset F$ , say, and  $D$  is  $F$ . But, in (1), when  $\mathcal{E} = [\_]N$ , even if we know that the redex has type  $F$  in  $\Gamma$ , and hence  $C = E \supset F$ , for some  $E$ ,  $D$  need not be  $F$ , in which case the contractum would not have type  $F$  in  $\Gamma$ .

If we wanted to constrain (1) to become equal to  $\pi$ , we would define it only for certain pairs  $(\mathcal{E}, C)$ , with  $D = D(\mathcal{E}, C)$  determined by  $(\mathcal{E}, C)$  as follows:

- $D([\_]N, E \supset F) = F$ ;
- $D([\_]i, C_1 \wedge C_2) = C_i$ , for  $i = 1, 2$ ;
- $D(\text{case}([\_], x^A.P, y^B.Q, E), A \vee B) = E$ ;
- $D(\text{abort}([\_], E), \perp) = E$ .<sup>3</sup>

Similar remarks apply to  $\varpi$  versus  $\mathcal{E}[\text{abort}(M, C)] \rightarrow \text{abort}(M, D)$ .

For instance,  $R$  is compatible with the application constructor if  $M R M'$  implies  $(MN) R (M'N)$ , and  $N R N'$  implies  $(MN) R (MN')$ .

<sup>3</sup>Curiously, if the proof terms had been defined without the last type parameter in *case*- and *abort*-expressions, then the version of (1) without  $C$  and  $D$  would determine a reduction relation  $\rightarrow$  enjoying subject reduction.

Figure 3: Reduction rules

Detour conversion rules:

$$\begin{array}{ll}
 (\beta_{\supset}) & (\lambda x.M)N \rightarrow [N/x]M \\
 (\beta_{\wedge}) & \langle M_1, M_2 \rangle i \rightarrow M_i \quad (i = 1, 2) \\
 (\beta_{\vee}) & \text{case}(\text{in}_i(M, A_1, A_2), x_1^{A_1}.P_1, x_2^{A_2}.P_2) \rightarrow [M/x_i]P_i \quad (i = 1, 2)
 \end{array}$$

Commutative conversion rules for disjunction (in the 2nd rule,  $i \in \{1, 2\}$ ):

$$\begin{array}{ll}
 (\pi_{\supset}) & (\text{case}(M, x.P, y.Q, C \supset D))N \rightarrow \text{case}(M, x.PN, y.QN, D) \\
 (\pi_{\wedge}) & (\text{case}(M, x.P, y.Q, C_1 \wedge C_2))i \rightarrow \text{case}(M, x.Pi, y.Qi, Ci) \\
 (\pi_{\vee}) & \text{case}(\text{case}(M, x'.P', y'.Q', C \vee D), x^C.P, y^D.Q, E) \rightarrow \\
 & \text{case}(M, x'.\text{case}(P', x^C.P, y^D.Q, E), y'.\text{case}(Q', x^C.P, y^D.Q, E), E) \\
 (\pi_{\perp}) & \text{abort}(\text{case}(M, x.P, y.Q, \perp), C) \rightarrow \\
 & \text{case}(M, x.\text{abort}(P, C), y.\text{abort}(Q, C), C)
 \end{array}$$

Commutative conversion rules for absurdity (in the 2nd rule,  $i \in \{1, 2\}$ ):

$$\begin{array}{ll}
 (\varpi_{\supset}) & (\text{abort}(M, C \supset D))N \rightarrow \text{abort}(M, D) \\
 (\varpi_{\wedge}) & (\text{abort}(M, C_1 \wedge C_2))i \rightarrow \text{abort}(M, Ci) \\
 (\varpi_{\vee}) & \text{case}(\text{abort}(M, C \vee D), x^C.P, y^D.Q, E) \rightarrow \text{abort}(M, E) \\
 (\varpi_{\perp}) & \text{abort}(\text{abort}(M, \perp), C) \rightarrow \text{abort}(M, C)
 \end{array}$$

$\eta$ -rules:

$$\begin{array}{ll}
 (\eta_{\supset}) & \lambda x.Mx \rightarrow M \quad (x \notin M) \\
 (\eta_{\wedge}) & \langle M1, M2 \rangle \rightarrow M \\
 (\eta_{\vee}) & \text{case}(M, x^A.\text{in}_1(x, A, B), y^B.\text{in}_2(y, A, B), A \vee B) \rightarrow M
 \end{array}$$

## System **F**

We give a precise definition of the polymorphic system **F** by saying what changes relatively to **IPC** (for an introduction to system **F**, see [7]). In the spirit of the Curry-Howard correspondence, we sometimes refer to **F** as the natural deduction system **NI**<sup>2</sup>.

Regarding formulas,  $\perp$  and  $A \vee B$  are dropped, and the new form  $\forall X.A$  is adopted (hence conjunction is taken as primitive in system **F**). The quantifier  $\forall X$  binds free occurrences of  $X$ , inducing the obvious concept of free occurrence of a type variable in a type. Concerning  $\alpha$ -equivalence, we deal with type variables as we deal with term variables, relying on silent  $\alpha$ -renaming. We write  $X \notin A$  to say that  $X$  does not occur free in  $A$ ; given the silent  $\alpha$ -renaming in  $A$ , we may assume  $X$  does not occur bound in  $A$  either. Another novelty, distinctive of system **F**, is type substitution in types,  $[B/X]A$ , meaning: substitution in  $A$  of each free occurrence of  $X$  by the type  $B$ .

Regarding proof terms, the constructions relative to  $\perp$  and  $A \vee B$  are dropped, and

the new forms  $\Lambda X.M$  and  $MB$ , with  $B$  a type, are added. The latter gives rise to a new form of evaluation contexts:  $\mathcal{E} ::= [\_ ]B$ .

Regarding typing rules, those relative to  $\perp$  and  $A \vee B$  are dropped, and two rules relative to  $\forall X.A$  are adopted:

$$\frac{\Gamma \vdash M : A}{\Gamma \vdash \Lambda X.M : \forall X.A} \forall I \quad \frac{\Gamma \vdash M : \forall X.A}{\Gamma \vdash MB : [B/X]A} \forall E$$

where the proviso for  $\forall I$  is:  $X$  occurs free in no type in  $\Gamma$ . Due to rule  $\forall E$ , the construction  $MB$  is called *universal instantiation*.

The new form of elimination contexts  $\mathcal{E}_\forall$  is typed with:

$$\overline{\Gamma | \forall X.A \vdash [\_]B : [B/X]A}$$

Regarding reduction rules, we drop commuting conversion rules (since they are relative to  $\vee$  and  $\perp$ ). What remains are the  $\beta$  and  $\eta$ -rules (but we drop those relative to disjunction). For  $\forall$ , these are:

$$\begin{array}{ll} (\beta_\forall) & (\Lambda X.M)B \rightarrow [B/X]M \\ (\eta_\forall) & \Lambda X.MX \rightarrow M \quad (X \notin M) \end{array}$$

We let  $\beta := \beta_\supset \cup \beta_\wedge \cup \beta_\forall$ . Similarly for  $\eta$ .

### System $\mathbf{F}_{\text{at}}$

The atomic polymorphic system  $\mathbf{F}_{\text{at}}$ , is the fragment of system  $\mathbf{F}$  induced by restricting to atomic instances the elimination inference rule for  $\forall$ , and the corresponding proof term constructor.

Thus the types/formulas of  $\mathbf{F}_{\text{at}}$  are exactly the types of  $\mathbf{F}$  with type substitution in types only required in the atomic form  $[Y/X]A$  and the proof terms of  $\mathbf{F}_{\text{at}}$  only differ from the proof terms of  $\mathbf{F}$  in the construction relatively to  $\forall E$  being  $MB$  replaced by  $MX$  which gives rise to  $\mathcal{E}_\forall ::= [\_]X$ .

The typing rules relatively to  $\forall X.A$  are:

$$\frac{\Gamma \vdash M : A}{\Gamma \vdash \Lambda X.M : \forall X.A} \forall I \quad \frac{\Gamma \vdash M : \forall X.A}{\Gamma \vdash MX : [Y/X]A} \forall E_{\text{at}}$$

where the proviso for  $\forall I$  is:  $X$  occurs free in no type in  $\Gamma$ . The new form of elimination contexts  $\mathcal{E}_\forall$  is typed with:

$$\overline{\Gamma | \forall X.A \vdash [\_]Y : [Y/X]A}$$

The reduction rules for  $\forall$  are:

$$\begin{array}{ll} (\beta_\forall) & (\Lambda X.M)Y \rightarrow [Y/X]M \\ (\eta_\forall) & \Lambda X.MX \rightarrow M \quad (X \notin M) \end{array}$$

### 3 The Russell-Prawitz embedding

We recall the Russell-Prawitz translation of **IPC** into **F**. The treatment is by means of proof terms rather than derivations. In this section we just define the translation, observe type soundness, and revisit [10] to justify the designation “Russell-Prawitz”. The matter of preservation of proof reduction is postponed to the next section.

**Definition 1.** *In **F** (and in **F<sub>at</sub>**):*

1.  $A \underline{\vee} B := \forall X.((A \supset X) \wedge (B \supset X)) \supset X$ , with  $X \notin A, B$ .
2.  $\underline{\perp} := \forall X.X$ .

We define the Russell-Prawitz translation of formulas. Using the abbreviations just introduced, the definition can be given in a homomorphic fashion:

$$\begin{aligned} X^\bullet &= X \\ \underline{\perp}^\bullet &= \underline{\perp} \\ (A \supset B)^\bullet &= A^\bullet \supset B^\bullet \\ (A \wedge B)^\bullet &= A^\bullet \wedge B^\bullet \\ (A \vee B)^\bullet &= A^\bullet \underline{\vee} B^\bullet \end{aligned}$$

The translation of proof terms will rely on the following definition:

**Definition 2.** *In **F**:*

1. Given  $M, A, B$ , given  $i \in \{1, 2\}$ , we define

$$\underline{\text{IN}}_i(M, A, B) := \Lambda X. \lambda w^{(A \supset X) \wedge (B \supset X)}. w i M,$$

where the bound variable  $X$  is chosen so that  $X \notin M, A, B$ .

2. Given  $M, P, Q, A, B, C$ , we define

$$\underline{\text{CASE}}(M, x^A.P, y^B.Q, C) := MC \langle \lambda x^A.P, \lambda y^B.Q \rangle$$

3. Given  $M, A$ , we define  $\underline{\text{ABORT}}(M, A) := MA$

It is straightforward to see that the typing rules in Fig. 4 - that is, the inference rules for disjunction and absurdity - are derivable in **F**.

The following result is also straightforward:

**Lemma 1.** *Let  $R$  be a relation compatible in the proof-terms of **F**. Then the compatibility rules in Fig. 5 are derivable in **F**.*

Due to Definition 2, the translation of proof terms can be given in a purely homomorphic fashion:

**Definition 3.** *Given  $M \in \text{IPC}$ ,  $M^\bullet$  is defined by recursion on  $M$  as in Fig. 6.*



Figure 4: Derivable typing rules of **F**

$$\begin{array}{c}
\frac{\Gamma \vdash M : A_i}{\Gamma \vdash \underline{\text{IN}}_i(M, A_1, A_2) : A_1 \vee A_2} \quad (i = 1, 2) \\
\\
\frac{\Gamma \vdash M : A \vee B \quad \Gamma, x : A \vdash P : C \quad \Gamma, y : B \vdash Q : C}{\Gamma \vdash \underline{\text{CASE}}(M, x^A.P, y^B.Q, C) : C} \\
\\
\frac{\Gamma \vdash M : \perp}{\Gamma \vdash \underline{\text{ABORT}}(M, C) : C}
\end{array}$$

Figure 5: Derivable compatibility rules of **F**

$$\begin{array}{c}
\frac{M \ R \ M'}{\underline{\text{IN}}_i(M, A, B) \ R \ \underline{\text{IN}}_i(M', A, B)} \\
\\
\frac{M \ R \ M'}{\underline{\text{CASE}}(M, x.P, y.Q, C) \ R \ \underline{\text{CASE}}(M', x.P, y.Q, C)} \\
\\
\frac{P \ R \ P'}{\underline{\text{CASE}}(M, x.P, y.Q, C) \ R \ \underline{\text{CASE}}(M, x.P', y.Q, C)} \\
\\
\frac{Q \ R \ Q'}{\underline{\text{CASE}}(M, x.P, y.Q, C) \ R \ \underline{\text{CASE}}(M, x.P, y.Q', C)} \\
\\
\frac{M \ R \ M'}{\underline{\text{ABORT}}(M, C) \ R \ \underline{\text{ABORT}}(M', C)}
\end{array}$$

Notice that  $(MN)^\bullet = M^\bullet N^\bullet$  and  $(Mi)^\bullet = M^\bullet i$ .

Observe the use of the type information provided by the last argument of case- and abort-expressions: from  $C$  in  $\text{case}(M, x^A.P, y^B.Q, C)$  we determine the argument  $C^\bullet$  required by  $\underline{\text{CASE}}$ ; from  $A$  in  $\text{abort}(M, A)$  we determine the argument  $A^\bullet$  for  $\underline{\text{ABORT}}$ .<sup>4</sup>

**Proposition 1** (Type soundness). *If  $\Gamma \vdash M : A$  in **IPC**, then  $\Gamma^\bullet \vdash M^\bullet : A^\bullet$  in **F**.*

The easy proof of this proposition determines a transformation of derivations in **IPC** into derivations in **F**, a transformation defined by recursion on the given derivation in **IPC**, based on the derivability in **F** of each inference rule of **IPC**.

We now argue that such a transformation is already implicit in [10]. For this discussion, let disjunction be a primitive connective of **NI**<sup>2</sup> (here, contrary to [10], we will ignore the second-order existential quantifier). This corresponds to extending system **F** with the type former  $A \vee B$  and the constructions  $\text{in}_i(M, A, B)$  ( $i = 1, 2$ ) and

<sup>4</sup>If the proof terms of **IPC** had been defined without the last type parameter in case- and abort-expressions, instead of a translation of proof terms, we would have a translation of typing derivations.

Figure 6: The Russell-Prawitz translation of proof expressions

$$\begin{aligned}
x^\bullet &= x \\
(\lambda x^A.M)^\bullet &= \lambda x^{A^\bullet}.M^\bullet \\
\langle M, N \rangle^\bullet &= \langle M^\bullet, N^\bullet \rangle \\
(\text{in}_i(M, A, B))^\bullet &= \underline{\text{IN}}_i(M^\bullet, A^\bullet, B^\bullet) \\
(\mathcal{E}[M])^\bullet &= \mathcal{E}^\bullet[M^\bullet] \\
(\text{case}(M, x^A.P, y^B.Q, C))^\bullet &= \underline{\text{CASE}}(M^\bullet, x^{A^\bullet}.P^\bullet, y^{B^\bullet}.Q^\bullet, C^\bullet) \\
(\text{abort}(M, A))^\bullet &= \underline{\text{ABORT}}(M^\bullet, A^\bullet) \\
([\_]N)^\bullet &= [\_]N^\bullet \\
([\_]i)^\bullet &= [\_]i
\end{aligned}
\tag{$i = 1, 2$}$$

$\text{case}(M, x^A.P, y^B.Q, C)$ . Prawitz [10] shows that in  $\mathbf{NI}^2$  the connectives  $\wedge$ ,  $\vee$  and  $\perp$  are definable operations. For instance, in the case of disjunction, this means that  $(A_1 \vee A_2) \supset (A_1 \underline{\vee} A_2)$  and  $(A_1 \underline{\vee} A_2) \supset (A_1 \vee A_2)$  are theorems of  $\mathbf{NI}^2$ . The proof in [10], in terms of the extended system  $\mathbf{F}$ , amounts to the following derivable sequents:

$$y : A_1 \vee A_2 \vdash \Lambda X \lambda w^{(A_1 \supset X) \wedge (A_2 \supset X)}. \text{case}(y, x_1.w1x_1, x_2.x_2, w2x_2) : A_1 \underline{\vee} A_2 \quad (2)$$

$$z : A_1 \underline{\vee} A_2 \vdash z(A_1 \vee A_2) \langle \lambda x_1. \text{in}_1(x_1, A_1, A_2), \lambda x_2. \text{in}_2(x_2, A_1, A_2) \rangle : A_1 \vee A_2 \quad (3)$$

This is very close to show the admissibility of the introduction and elimination rules for  $A_1 \vee A_2$  (the first two rules of Fig. 4). Given  $\Gamma \vdash M : A_i$ , from (2) we get

$$\Gamma \vdash \Lambda X \lambda w^{(A_1 \supset X) \wedge (A_2 \supset X)}. \text{case}(\text{in}_i(M, A_1, A_2), x_1.w1x_1, x_2.x_2, w2x_2) : A_1 \underline{\vee} A_2$$

Applying  $\beta_\vee$ , the term reduces to  $\Lambda X \lambda w^{(A_1 \supset X) \wedge (A_2 \supset X)}. wiM$ . On the other hand, given  $\Gamma, x_i : A_i \vdash P_i : C$ , for  $i = 1, 2$ , a variation of (3) gives

$$\Gamma, z : A_1 \underline{\vee} A_2 \vdash zC \langle \lambda x_1. P_1, \lambda x_2. P_2 \rangle : C$$

So, if we are further given  $\Gamma \vdash M : A_1 \underline{\vee} A_2$ , we obtain

$$\Gamma \vdash MC \langle \lambda x_1. P_1, \lambda x_2. P_2 \rangle : C$$

## 4 Atomization of universal instantiation

In this section we add to system  $\mathbf{F}$  extra conversions  $\varrho$  and  $\rho$  which promote the atomization of universal instantiation. We show that typable terms have unique “atomic” normal forms. We also propose new conversions  $\varepsilon$  and  $\epsilon$ , which postulate the commuting principles for the derived connectives of disjunction and absurdity, and which are simple variants of a general commuting principle introduced in [11]<sup>5</sup>. The latter

<sup>5</sup>Notice, however, that here, contrary to [11], in the formulation of the commuting principles  $\varepsilon$  and  $\epsilon$ , we do not constraint ourselves to formulas obeying certain restrictions in the polarity of the occurrences of type variables.

principle adds “naturality” to natural deduction, according to [11]. Here we work out in detail the relationship of  $\varepsilon$  and  $\epsilon$  with a more general “dinaturality” principle. The relationship between  $\varrho$ ,  $\rho$  and  $\varepsilon$ ,  $\epsilon$  is also worked out. Since it has been proved that adding the dinaturality principle to system **F** does not make the system inconsistent [2], the same follows with respect to  $\varepsilon$  and  $\epsilon$ . We profit from the relationship among all the new conversions to prove that extending system **F** with  $\varrho$  and  $\rho$  does not bring inconsistency. We also show the simulation theorem for the Russell-Prawitz translation, which makes use of the atomization conversions.

#### 4.1 New conversions for system **F**

The  $\varrho$ - and  $\rho$ -redexes are terms of the form  $\text{CASE}(M, x.P, y.Q, C)$  and  $\text{ABORT}(M, C)$ , respectively, where  $C$  is not atomic. Therefore, such redexes include a universal instantiation with a non-atomic formula  $C$ . The common purpose of each of the  $\varrho$ - and  $\rho$ -conversion rules is to replace one such instantiation by another with a sub-formula of  $C$ . Since there is a common purpose, the two conversion rules are denoted with symbols “ $\varrho$ ” and “ $\rho$ ” which are variant of each other.

**Definition 4** (Atomization conversion rules in **F**). 1. A  $\varrho$ -redex is a term of the form  $MC\langle\lambda x^A.P, \lambda y^B.Q\rangle$ , where  $C$  is not atomic. There are three  $\varrho$ -conversion rules for this redex, depending on the form of  $C$ :

$$\begin{aligned} M(C_1 \supset C_2)\langle\lambda x^A.P, \lambda y^B.Q\rangle &\rightarrow \lambda z^{C_1}.MC_2\langle\lambda x^A.Pz, \lambda y^B.Qz\rangle \\ M(C_1 \wedge C_2)\langle\lambda x^A.P, \lambda y^B.Q\rangle &\rightarrow \langle MC_i\langle\lambda x^A.Pi, \lambda y^B.Qi\rangle\rangle_{i=1,2} \\ M(\forall Y.D)\langle\lambda x^A.P, \lambda y^B.Q\rangle &\rightarrow \Lambda Y.MD\langle\lambda x^A.PY, \lambda y^B.QY\rangle \end{aligned}$$

where  $z \neq x$ ,  $z \neq y$ ,  $z \notin P, Q, M$ ; and  $Y \notin P, Q, M, A, B$ .

2. A  $\rho$ -redex is a term of the form  $MC$ , where  $C$  is not atomic. There are three  $\rho$ -conversion rules for this redex, depending on the form of  $C$ :

$$\begin{aligned} M(C_1 \supset C_2) &\rightarrow \lambda z^{C_1}.MC_2 \\ M(C_1 \wedge C_2) &\rightarrow \langle MC_i\rangle_{i=1,2} \\ M(\forall Y.D) &\rightarrow \Lambda Y.MD \end{aligned}$$

where  $z \notin M$ ; and  $Y \notin M$ .

For now, a  $\varrho$ -redex always contains a  $\rho$ -redex. Typing constraints will later forbid this situation. However, typing considerations for these rules and the discussion of subject reduction are postponed to Subsection 4.3.

We now introduce a variant of the atomization conversion  $\varrho$ .

**Definition 5.** The  $\delta$ -conversion rules are as follows:

$$\begin{aligned} M(C_1 \supset C_2)\langle\lambda x^A.\lambda z^{C_1}.P, \lambda y^B.\lambda z^{C_1}.Q\rangle &\rightarrow \lambda z^{C_1}.MC_2\langle\lambda x^A.P, \lambda y^B.Q\rangle \\ M(C_1 \wedge C_2)\langle\lambda x^A.\langle P_i\rangle_{i=1,2}, \lambda y^B.\langle Q_i\rangle_{i=1,2}\rangle &\rightarrow \langle MC_i\langle\lambda x^A.P_i, \lambda y^B.Q_i\rangle\rangle_{i=1,2} \\ M(\forall Y.D)\langle\lambda x^A.\Lambda Y.P, \lambda y^B.\Lambda Y.Q\rangle &\rightarrow \Lambda Y.MD\langle\lambda x^A.P, \lambda y^B.Q\rangle \end{aligned}$$

A  $\delta$ -redex is a particular form of  $\varrho$ -redex which, if reduced by  $\varrho$ , generates two  $\beta$ -redexes (actually four, in the case of conjunction). If these are reduced away immediately, we obtain the effect of  $\delta$ -reduction. Conversely, a  $\varrho$ -redex, if  $\eta$ -expanded, can be reduced with  $\delta$  instead of  $\varrho$ . So,  $\delta$  and  $\varrho$  are related via  $\beta\eta$ -conversions, as the next result shows.

**Proposition 2** (Variants of atomization). *Let  $M, N \in \mathbf{F}$ .*

1. *If  $M \rightarrow_\delta N$  then  $M \rightarrow_{\varrho\beta}^+ N$ .*
2. *If  $M \rightarrow_\varrho N$  then  $M =_{\delta\eta} N$ .*

*Proof.* We have to do an induction on  $M \rightarrow_\delta N$  and another on  $M \rightarrow_\varrho N$ . In both proofs, the inductive cases are routine because the relations  $\rightarrow_{\varrho\beta}^+$  and  $=_{\delta\eta}$  are compatible. In each proof there are 3 base cases. We just illustrate with two base cases for the first assertion and one for the second.

$$\begin{aligned}
& M(C \supset D) \langle \lambda x^A \lambda z^C . P, \lambda y^B \lambda z^C . Q \rangle \\
& \rightarrow_{\varrho} \lambda w^C . MD \langle \lambda x^A . (\lambda z^C . P) w, \lambda y^B . (\lambda z^C . Q) w \rangle \\
& \xrightarrow{\beta} \lambda w^C . MD \langle \lambda x^A . [w/z] P, \lambda y^B . [w/z] Q \rangle \\
& = \lambda z^C . MD \langle \lambda x^A . P, \lambda y^B . Q \rangle \\
\\
& M(\forall Y . D) \langle \lambda x^A \Lambda Y . P, \lambda y^B \Lambda Y . Q \rangle \\
& = M(\forall Y . D) \langle \lambda x^A \Lambda Z . [Z/Y] P, \lambda y^B \Lambda Z . [Z/Y] Q \rangle \\
& \xrightarrow{\varrho} \Lambda Y . MD \langle \lambda x^A . (\Lambda Z . [Z/Y] P) Y, \lambda y^B . (\Lambda Z . [Z/Y] Q) Y \rangle \\
& \xrightarrow{\beta} \Lambda Y . MD \langle \lambda x^A . P, \lambda y^B . Q \rangle \\
\\
& M(C_1 \wedge C_2) \langle \lambda x^A . P, \lambda y^B . Q \rangle \\
& \leftarrow_{\eta} M(C_1 \wedge C_2) \langle \lambda x^A . \langle Pi \rangle_{i=1,2}, \lambda y^B . \langle Qi \rangle_{i=1,2} \rangle \\
& \rightarrow_{\delta} \langle MC_i \langle \lambda x^A . Pi, \lambda y^B . Qi \rangle \rangle_{i=1,2}
\end{aligned}$$

□

According to the previous result, a  $\delta$ -reduction step can be broken into a  $\varrho\beta$ -reduction sequence, but a  $\varrho$ -reduction step can be derived only as a  $\delta\eta$ -equality. Given our insistence on reduction, rather than mere equality, in the main results to be shown below, the previous result is an argument to take the  $\varrho$ -conversion rules as primitive, instead of the  $\delta$ -conversion rules.

The  $\delta$ -conversions pull down an introduction inference with which the two branches  $P$  and  $Q$  of a  $\underline{\text{CASE}}(M, x.P, y.Q, C)$  end. Dually, a commuting conversion pushes up to the two branches  $P$  and  $Q$  of a  $\underline{\text{CASE}}(M, x.P, y.Q, C)$  an elimination inference of which the mentioned  $\underline{\text{CASE}}$  is main premiss.

**Definition 6** (Commuting conversion rules in  $\mathbf{F}$ ).

1. *The  $\varepsilon$ -conversion rules are as follows:*

$$\begin{aligned}
M(C_1 \supset C_2) \langle \lambda x^A . P, \lambda y^B . Q \rangle N & \rightarrow MC_2 \langle \lambda x^A . PN, \lambda y^B . QN \rangle \\
M(C_1 \wedge C_2) \langle \lambda x^A . P, \lambda y^B . Q \rangle i & \rightarrow MC_i \langle \lambda x^A . Pi, \lambda y^B . Qi \rangle \\
M(\forall Y . C') \langle \lambda x^A . P, \lambda y^B . Q \rangle C'' & \rightarrow M([C''/Y]C') \langle \lambda x^A . PC''', \lambda y^B . QC''' \rangle
\end{aligned}$$

2. The  $\epsilon$ -conversion rules are as follows:

$$\begin{aligned} M(C_1 \supset C_2)N &\rightarrow MC_2 \\ M(C_1 \wedge C_2)i &\rightarrow MC_i \\ M(\forall Y.C')C'' &\rightarrow M([C''/Y]C') \end{aligned}$$

We leave it to the reader to rewrite these rules in terms of CASE and ABORT.

Recall the discussion on how to define commutative conversions in **IPC**. In **F**,  $\varepsilon$  is strictly contained in the following auxiliary rule:

$$(\varepsilon') \quad \mathcal{E}[\underline{\text{CASE}}(M, x^A.P, y^B.Q, C)] \rightarrow \underline{\text{CASE}}(M, x^A.\mathcal{E}[P], y^B.\mathcal{E}[Q], D) .$$

The two rules are not the same due to the fact that in  $\varepsilon'$  no connections is imposed on  $C$  and  $D$ . If we wanted to constrain this rule to become equal to  $\varepsilon$ , we would define it only for certain pairs  $(\mathcal{E}, C)$ , with  $D = D(\mathcal{E}, C)$  determined by  $(\mathcal{E}, C)$  as follows:

$$\begin{aligned} D([\_]N, E \supset F) &= F \\ D([\_]i, C_1 \wedge C_2) &= C_i \quad (i = 1, 2) \\ D([\_]E, \forall X.C_0) &= [E/X]C_0 \end{aligned} \tag{4}$$

Similar remarks apply to  $\epsilon$  versus the auxiliary rule

$$(\epsilon') \quad \mathcal{E}[\underline{\text{ABORT}}(M, C)] \rightarrow \underline{\text{ABORT}}(M, D) .$$

Commutative conversions rules are named with symbols “ $\varepsilon$ ” and “ $\epsilon$ ”, which are a variant of each other, again as a reminder that they express related commuting principles. That relation will be even more evident when reducing typable terms; but, as before with atomization and  $\delta$ , we postpone to Subsection 4.3 all considerations about subject reduction and typing in connection with commutative conversions.

In all cases of the  $\varepsilon$ - and  $\epsilon$ -conversion rules, a universal instantiation with formula  $C$  is replaced by another with some formula  $D$ , and in all cases  $D$  is a sub-formula of  $C$ , except when  $C = \forall Y.C'$  and  $\mathcal{E} = [\_]C''$ , for some formulas  $C'$  and  $C''$ , in which case  $D = [C''/Y]C'$ . Let us compare  $\varrho$  with  $\varepsilon$  in this situation:

$$\begin{aligned} \underline{\text{CASE}}(M, x.P, y.Q, \forall Y.C') &\rightarrow_{\varrho} \Lambda Y.\underline{\text{CASE}}(M, x.PY, y.QY, C') \\ \underline{\text{CASE}}(M, x.P, y.Q, \forall Y.C')C'' &\rightarrow_{\varepsilon} \underline{\text{CASE}}(M, x.PC'', y.QC'', [C''/Y]C') \end{aligned}$$

Starting from the  $\varepsilon$ -redex, an obvious alternative is to apply, not rule  $\varepsilon$ , but rule  $\varrho$  instead, to reach the intermediate term  $(\Lambda Y.\underline{\text{CASE}}(M, x.PY, y.QY, C'))C''$ . The effect of  $\varepsilon$ -reduction is obtained by a further  $\beta$ -reduction step. In fact, each  $\varepsilon$ - and  $\epsilon$ -reduction step has a similar decomposition, as the first two items of the next result show.

**Proposition 3** (Atomization vs commuting conversion). *Let  $M, N \in \mathbf{F}$ .*

1. *If  $M \rightarrow_{\varepsilon} N$  then  $M \rightarrow_{\varrho\beta}^2 N$ .*
2. *If  $M \rightarrow_{\epsilon} N$  then  $M \rightarrow_{\rho\beta}^2 N$ .*
3. *If  $M \rightarrow_{\varrho} N$  then  $M =_{\varepsilon\eta} N$ .*

4. If  $M \rightarrow_\rho N$  then  $M =_{\epsilon\eta} N$ .

*Proof.* We give four proofs by induction. We never show the inductive cases, which are routine.

The first assertion is proved by induction on  $M \rightarrow_\varepsilon N$ . There are three cases to consider, where the third corresponds to the discussion just before this proposition.

$$\begin{aligned}
M(C_1 \supset C_2) \langle \lambda x^A.P, \lambda y^B.Q \rangle N & \xrightarrow{\varrho} (\lambda z^{C_1}. MC_2 \langle \lambda x^A.Pz, \lambda y^B.Qz \rangle) N \\
& \xrightarrow{\beta} MC_2 \langle \lambda x^A.PN, \lambda y^B.QN \rangle \\
M(C_1 \wedge C_2) \langle \lambda x^A.P, \lambda y^B.Q \rangle i & \xrightarrow{\varrho} (\langle MC_j \langle \lambda x^A.Pj, \lambda y^B.Qj \rangle \rangle_{j=1,2}) i \\
& \xrightarrow{\beta} MC_i \langle \lambda x^A.Pi, \lambda y^B.Qi \rangle \\
M(\forall Y.C') \langle \lambda x^A.P, \lambda y^B.Q \rangle C'' & \xrightarrow{\varrho} (\Lambda Y. MC' \langle \lambda x^A.PY, \lambda y^B.QY \rangle) C'' \\
& \xrightarrow{\beta} M([C''/Y]C') \langle \lambda x^A.PC'', \lambda y^B.QC'' \rangle
\end{aligned}$$

For the second assertion, we proceed by induction on  $M \rightarrow_\rho N$ . The three cases of the base are proved by simple calculations.

$$\begin{aligned}
M(C_1 \supset C_2)N & \xrightarrow{\rho} (\lambda z^{C_1}. MC_2)N \xrightarrow{\beta} MC_2 \\
M(C_1 \wedge C_2)i & \xrightarrow{\rho} (\langle MC_j \rangle_{j=1,2})i \xrightarrow{\beta} MC_i \\
M(\forall Y.C')C'' & \xrightarrow{\rho} (\Lambda Y. MC')C'' \xrightarrow{\beta} M([C''/Y]C')
\end{aligned}$$

The third assertion is proved by induction on  $M \rightarrow_\varrho N$ . There are three base cases.

$$\begin{aligned}
M(C_1 \supset C_2) \langle \lambda x^A.P, \lambda y^B.Q \rangle & \xleftarrow{\eta} \lambda z^{C_1}. (M(C_1 \supset C_2) \langle \lambda x^A.P, \lambda y^B.Q \rangle) z \\
& \xrightarrow{\varepsilon} \lambda z^{C_1}. MC_2 \langle \lambda x^A.Pz, \lambda y^B.Qz \rangle \\
M(C_1 \wedge C_2) \langle \lambda x^A.P, \lambda y^B.Q \rangle & \xleftarrow{\eta} \langle (M(C_1 \wedge C_2) \langle \lambda x^A.P, \lambda y^B.Q \rangle) 1, (M(C_1 \wedge C_2) \langle \lambda x^A.P, \lambda y^B.Q \rangle) 2 \rangle \\
& \xrightarrow{\varepsilon} \langle MC_1 \langle \lambda x^A.P1, \lambda y^B.Q1 \rangle, MC_2 \langle \lambda x^A.P2, \lambda y^B.Q2 \rangle \rangle \\
& = \langle MC_i \langle \lambda x^A.Pi, \lambda y^B.Qi \rangle \rangle_{i=1,2} \\
M(\forall Y.C_0) \langle \lambda x^A.P, \lambda y^B.Q \rangle & \xleftarrow{\eta} \Lambda X. (M(\forall Y.C_0) \langle \lambda x^A.P, \lambda y^B.Q \rangle) X \\
& \xrightarrow{\varepsilon} \Lambda X. M([X/Y]C_0) \langle \lambda x^A.PX, \lambda y^B.QX \rangle \\
& = \Lambda Y. MC_0 \langle \lambda x^A.PY, \lambda y^B.QY \rangle
\end{aligned}$$

For the fourth assertion, the calculations of the base of the proof by induction on  $M \rightarrow_\rho N$  are as follows.

$$\begin{aligned}
M(C \supset D) & \xleftarrow{\eta} \lambda z^C. (M(C \supset D))z \xrightarrow{\varepsilon} \lambda z^C. MD \\
M(C_1 \wedge C_2) & \xleftarrow{\eta} \langle (M(C_1 \wedge C_2))1, (M(C_1 \wedge C_2))2 \rangle \xrightarrow{\varepsilon} \langle MC_1, MC_2 \rangle \\
M(\forall Y.C_0) & \xleftarrow{\eta} \Lambda X. (M(\forall Y.C_0))X \xrightarrow{\varepsilon} \Lambda X. M[X/Y]C_0
\end{aligned}$$

Notice  $\Lambda X. M[X/Y]C_0 = \Lambda Y. MC_0$  as required.  $\square$

In the same way as Prop. 2 is an argument to take  $\varrho$ -conversion rules as primitive, instead of the  $\delta$ -conversion rules, Prop. 3 is an argument to take the  $\varrho$ -conversion rules (respectively the  $\rho$ -conversion rules) as primitive instead of the  $\varepsilon$ -conversion rules (respectively the  $\epsilon$ -conversion rules). As a consequence, we may state below results in terms of  $\varepsilon\epsilon\delta$ -reduction, knowing that they may be immediately restated in terms of  $\varrho\rho$ -reduction, in view of Props. 2 and 3 – see for instance Theorem 1 below.

## 4.2 Strict simulation

It has been observed [5, 11] that the Russell-Prawitz translation does not yield a simulation of proof reduction. Next we show that, once  $\mathbf{F}$  is added  $\varrho\rho$ -conversions, a simulation of proof reduction occurs. The simulation is even *strict*, in the sense that each reduction step in  $\mathbf{IPC}$  is mapped to a non-empty reduction sequence in the enriched system  $\mathbf{F}$ .

**Theorem 1** (Strict simulation). *If  $M_1 \rightarrow M_2$  in  $\mathbf{IPC}$  then  $M_1^\bullet \rightarrow_{\beta\eta\epsilon\delta}^+ M_2^\bullet$  in  $\mathbf{F}$  (hence  $M_1^\bullet \rightarrow_{\beta\eta\varrho\rho}^+ M_2^\bullet$  in  $\mathbf{F}$ ). More precisely:*

- Case  $R \in \{\beta_\sup, \eta_\sup, \beta_\wedge, \eta_\wedge\}$ . If  $M_1 \rightarrow_R M_2$  in  $\mathbf{IPC}$  then  $M_1^\bullet \rightarrow_R M_2^\bullet$  in  $\mathbf{F}$ .
- Case  $R = \beta_\vee$ . If  $M_1 \rightarrow_R M_2$  in  $\mathbf{IPC}$  then  $M_1^\bullet \rightarrow_{\beta}^+ M_2^\bullet$  in  $\mathbf{F}$ .
- Case  $R = \eta_\vee$ . If  $M_1 \rightarrow_R M_2$  in  $\mathbf{IPC}$  then  $M_1^\bullet \rightarrow_{\eta\delta}^+ M_2^\bullet$  in  $\mathbf{F}$ .
- Case  $R \in \{\pi_\sup, \pi_\wedge, \pi_\vee, \pi_\perp\}$ . If  $M_1 \rightarrow_R M_2$  in  $\mathbf{IPC}$  then  $M_1^\bullet \rightarrow_{\epsilon}^+ M_2^\bullet$  in  $\mathbf{F}$ .
- Case  $R \in \{\varpi_\sup, \varpi_\wedge, \varpi_\vee, \varpi_\perp\}$ . If  $M_1 \rightarrow_R M_2$  in  $\mathbf{IPC}$  then  $M_1^\bullet \rightarrow_{\epsilon}^+ M_2^\bullet$  in  $\mathbf{F}$ .

*Proof.* For each rule  $R$  of  $\mathbf{IPC}$ , one does an induction on  $M_1 \rightarrow_R M_2$ . In each proof, the inductive cases follow routinely by induction hypothesis, since the various relations  $\rightarrow_S$  and  $\rightarrow_S^+$  in  $\mathbf{F}$ , with  $S \in \{\beta, \eta, \epsilon, \delta, \eta\delta\}$ , are compatible; and the base case corresponds to the reduction rule  $R$ . The base cases relative to reduction rules pertaining to  $\sup$  and  $\wedge$  are trivial because  $(\cdot)^\bullet$  maps the constructions pertaining to these connectives in homomorphic fashion, and because  $([N/x]M)^\bullet = [N^\bullet/x]M^\bullet$ . We detail the base cases relative to reduction rules pertaining to  $\vee$  and  $\perp$ .

Case  $\beta_\vee$ : We prove that  $\text{CASE}(\text{IN}_i(N, A_1, A_2), x_1^{A_1}.P_1, x_2^{A_2}.P_2, C) \rightarrow_{\beta}^+ [N/x_i]P_i$  in  $\mathbf{F}$ .

$$\begin{aligned}
 & \text{LHS} \\
 = & (\Lambda X. \lambda w^{(A_1 \sup X) \wedge (A_2 \sup X)}. wiN) C \langle \lambda x_1^{A_1}. P_1, \lambda x_2^{A_2}. P_2 \rangle \\
 \rightarrow_{\beta_\vee} & (\lambda w^{(A_1 \sup C) \wedge (A_2 \sup C)} wiN) \langle \lambda x_1^{A_1}. P_1, \lambda x_2^{A_2}. P_2 \rangle \\
 \rightarrow_{\beta_\sup} & \langle \lambda x_1^{A_1}. P_1, \lambda x_2^{A_2}. P_2 \rangle iN \\
 \rightarrow_{\beta_\wedge} & (\lambda x_i^{A_i}. P_i) N \\
 \rightarrow_{\beta_\sup} & [N/x_i] P_i
 \end{aligned}$$

The first equality is justified by the definitions of  $\text{CASE}$  and  $\text{IN}$ . To conclude the proof in this case, we need again the commutation of  $(\cdot)^\bullet$  with substitution.

Case  $\eta_\vee$ : We prove that  $\text{CASE}(M, x^A. \text{IN}_1(x, A, B), y^B. \text{IN}_2(y, A, B), A \vee B) \rightarrow_{\delta\eta}^+ M$  in  $\mathbf{F}$ .

$$\begin{aligned}
 & \text{LHS} \\
 = & M(A \vee B) \langle \lambda x^A \Lambda X \lambda w^{(A \sup X) \wedge (B \sup X)}. w1x, \lambda y^B \Lambda X \lambda w^{(A \sup X) \wedge (B \sup X)}. w2y \rangle \\
 \rightarrow_{\delta} & \Lambda X. M(((A \sup X) \wedge (B \sup X)) \sup X) \langle \lambda x^A. \lambda w. w1x, \lambda y^B. \lambda w. w2y \rangle \\
 \rightarrow_{\delta} & \Lambda X. \lambda w. M X \langle \lambda x^A. w1x, \lambda y^B. w2y \rangle \\
 \rightarrow_{\eta_\sup}^2 & \Lambda X. \lambda w. M X \langle w1, w2 \rangle \\
 \rightarrow_{\eta_\wedge} & \Lambda X. \lambda w. M X w \\
 \rightarrow_{\eta_\sup} & \Lambda X. M X \\
 \rightarrow_{\eta_\vee} & M
 \end{aligned}$$

The first equality is justified by the definitions of CASE and IN.

Cases  $\pi_{\supset}$  and  $\pi_{\wedge}$  follow immediately from a single application of  $\varepsilon$ . Just notice that, in **F**,  $(\underline{\text{CASE}}(M, x^A.P, y^B.Q, C \supset D))N \rightarrow_{\varepsilon} \underline{\text{CASE}}(M, x^A.PN, y^B.QN, D)$  and  $\underline{\text{CASE}}(M, x^A.P, y^B.Q, C_1 \wedge C_2)i \rightarrow_{\varepsilon} \underline{\text{CASE}}(M, x^A.Pi, y^B.Qi, C_i)$ .

Case  $\pi_{\vee}$ : We prove that, in **F**,

$$\begin{aligned} & \underline{\text{CASE}}(\underline{\text{CASE}}(M, x_1^{A_1}.P_1, x_2^{A_2}.P_2, B_1 \vee B_2), y_1^{B_1}.Q_1, y_2^{B_2}.Q_2, C) \rightarrow_{\varepsilon}^+ \\ & \quad \underline{\text{CASE}}(M, x_1^{A_1}.\underline{\text{CASE}}(P_1, y_1^{B_1}.Q_1, y_2^{B_2}.Q_2, C), x_2^{A_2}.\underline{\text{CASE}}(P_2, y_1^{B_1}.Q_1, y_2^{B_2}.Q_2, C), C). \end{aligned}$$

$$\begin{aligned} & LHS \\ = & (M(B_1 \vee B_2)\langle \lambda x_1^{A_1}.P_1, \lambda x_2^{A_2}.P_2 \rangle)C\langle \lambda y_1^{B_1}.Q_1, \lambda y_2^{B_2}.Q_2 \rangle \\ \rightarrow_{\varepsilon} & M(((B_1 \supset C) \wedge (B_2 \supset C)) \supset C)\langle \lambda x_1^{A_1}.P_1C, \lambda x_2^{A_2}.P_2C \rangle\langle \lambda y_1^{B_1}.Q_1, \lambda y_2^{B_2}.Q_2 \rangle \\ \rightarrow_{\varepsilon} & MC\langle \lambda x_1^{A_1}.P_1C\langle \lambda y_1^{B_1}.Q_1, \lambda y_2^{B_2}.Q_2 \rangle, \lambda x_2^{A_2}.P_2C\langle \lambda y_1^{B_1}.Q_1, \lambda y_2^{B_2}.Q_2 \rangle \rangle \\ = & RHS \end{aligned}$$

The definition of CASE justifies the equalities above.

Case  $\pi_{\perp}$ : In **F**, we have that

$$\underline{\text{ABORT}}(\underline{\text{CASE}}(M, x^A.P, y^B.Q, \perp), C) \rightarrow_{\varepsilon} \underline{\text{CASE}}(M, x^A.\underline{\text{ABORT}}(P, C), y^B.\underline{\text{ABORT}}(Q, C), C) .$$

Indeed:

$$LHS = (M\perp\langle \lambda x^A.P, \lambda y^B.Q \rangle)C \rightarrow_{\varepsilon} MC\langle \lambda x^A.PC, \lambda y^B.QC \rangle = RHS ,$$

where the two equalities are by definition of CASE and ABORT.

Cases  $\varpi_{\supset}$  and  $\varpi_{\wedge}$  follow immediately from a single application of  $\epsilon$ . Just notice that  $(\underline{\text{ABORT}}(M, A \supset B))N \rightarrow_{\epsilon} \underline{\text{ABORT}}(M, B)$  and  $\underline{\text{ABORT}}(M, C_1 \wedge C_2)i \rightarrow_{\epsilon} \underline{\text{ABORT}}(M, C_i)$ .

Case  $\varpi_{\vee}$ : We prove that, in **F**,

$$\underline{\text{CASE}}(\underline{\text{ABORT}}(M, A \vee B), x^A.P, y^B.Q, C) \rightarrow_{\epsilon}^+ \underline{\text{ABORT}}(M, C) .$$

$$\begin{aligned} & LHS \\ = & M(A \vee B)C\langle \lambda x^A.P, \lambda y^B.Q \rangle && \text{(by def. of } \underline{\text{CASE}} \text{ and } \underline{\text{ABORT}}) \\ \rightarrow_{\epsilon} & M((A \supset C) \wedge (B \supset C)) \supset C \rangle\langle \lambda x^A.P, \lambda y^B.Q \rangle \\ \rightarrow_{\epsilon} & MC \\ = & RHS && \text{(by def. of } \underline{\text{ABORT}}) \end{aligned}$$

Case  $\varpi_{\perp}$ : We prove, in **F**,

$$\underline{\text{ABORT}}(\underline{\text{ABORT}}(M, \perp), A) \rightarrow_{\epsilon} \underline{\text{ABORT}}(M, A) .$$

Observe that

$$LHS = M\perp A \rightarrow_{\epsilon} MA = RHS ,$$

where the two equalities are by definition of ABORT.  $\square$



Now suppose  $M_1 \rightarrow M_2$  in **IPC** and  $M_1$  is typable in  $\Gamma$ . By subject reduction,  $M_1$  and  $M_2$  have the same type ( $A$ , say) in  $\Gamma$ ,  $M_1$  and  $M_2$  can be seen as proofs of  $A$ , and the reduction step  $M_1 \rightarrow M_2$  can be seen as a normalization step between the proofs  $M_1$  and  $M_2$ . Moreover, we know  $M_1^\bullet$  and  $M_2^\bullet$  have type  $A^\bullet$  in  $\Gamma^\bullet$ , and the strict simulation theorem gives  $M_1^\bullet \rightarrow_{\beta\eta\varrho\rho}^+ M_2^\bullet$  in **F**: but does this reduction correspond to a sequence of normalization and atomization steps between successive proofs of  $A^\bullet$ ? To answer to this question, we have to investigate the typing of atomization (and  $\delta$ , and commutative) conversions.

### 4.3 Properties of typable atomization

We investigate atomization in connection with typing. Recall for instance the  $\varrho$ -conversion rule with  $C = C_1 \supset C_2$ :

$$M(C_1 \supset C_2) \langle \lambda x^A.P, \lambda y^B.Q \rangle \rightarrow \lambda z^{C_1}.MC_2 \langle \lambda x^A.Pz, \lambda y^B.Qz \rangle \quad (*)$$

From the assumption that the redex of  $(*)$  has type  $D$  in  $\Gamma$ , say, we *cannot* infer that the contractum has the same type in  $\Gamma$ . That is, the subject-reduction property fails, if the conversion rule is formulated solely as  $(*)$ . The preservation of type from redex to contractum is guaranteed if, additionally, we demand that  $M$  has type  $A \vee B$  in  $\Gamma$ .

Now, the ammended rule is *not* to take  $(*)$  together with the requirement that, for *some*  $\Gamma$ , the redex has a type and  $M$  has type  $A \vee B$ . Such rule (let alone its compatible closure) would still fail the subject-reduction test, because we could be given another  $\Gamma'$  in which the redex had some type, and again, in the case  $\Gamma'$  was not  $\Gamma$ , no guarantee would exist that the contractum had in  $\Gamma'$  the same type as the redex.

The ammended rule is to take  $(*)$  as defining a ternary relation, consisting of tuples  $(N, N', \Gamma)$  where  $N$  and  $N'$  are, respectively, a redex and its contractum according to  $(*)$ , and  $\Gamma$  is an environment in which  $M$  has type  $A \vee B$ . But, then, how to define the compatible closure of such ternary relation? We cannot simply close the pairs  $(N, N')$  under the term-forming operations, because the  $\Gamma$  may vary as we form new pairs - so the closure rules have to deal with  $\Gamma$  as well. In the end, we will have another set of tuples  $(N, N', \Gamma)$ , whose intuition is:  $N \rightarrow N'$  is fine in  $\Gamma$ . The preservation of type from redex to contractum, guaranteed above for the rule  $(*)$ , will hold now from  $N$  to  $N'$  - but only because the type is given in a fine  $\Gamma$ , not an arbitrary  $\Gamma'$ .

**Definition 7** (Fine Atomization). *Let  $\Gamma$  be an environment.*

1. A  $\varrho$ -redex  $MC \langle \lambda x^A.P, \lambda y^B.Q \rangle$  is fine in  $\Gamma$  if  $M$  has type  $A \vee B$  in  $\Gamma$ .
2. A  $\rho$ -redex  $MC$  is fine in  $\Gamma$  if  $M$  has type  $\perp$  in  $\Gamma$ .
3. A root  $\varrho\rho$ -reduction (an instance of the  $\varrho\rho$ -conversion rules) is fine in  $\Gamma$  if the redex is fine in  $\Gamma$ .
4. Let  $R \in \{\varrho, \rho, \varrho\rho\}$ . The fine root  $R$ -reductions define a ternary relation, namely

$$\mathcal{R} := \{(M, M', \Gamma) \mid M \rightarrow M' \text{ is a root } R\text{-reduction fine in } \Gamma\} .$$

Figure 7: Fine compatible closure rules

- (i) If  $M \rightarrow M'$  is fine in  $x : A, \Gamma$ , then  $\lambda x^A.M \rightarrow \lambda x^A.M'$  is fine in  $\Gamma$ .
- (ii) If  $M \rightarrow M'$  is fine in  $\Gamma$ , then  $MN \rightarrow M'N$  is fine in  $\Gamma$ .
- (iii) If  $N \rightarrow N'$  is fine in  $\Gamma$ , then  $MN \rightarrow MN'$  is fine in  $\Gamma$ .
- (iv) If  $M \rightarrow M'$  is fine in  $\Gamma$ , then  $\langle M, N \rangle \rightarrow \langle M', N \rangle$  is fine in  $\Gamma$ .
- (v) If  $N \rightarrow N'$  is fine in  $\Gamma$ , then  $\langle M, N \rangle \rightarrow \langle M, N' \rangle$  is fine in  $\Gamma$ .
- (vi) If  $M \rightarrow M'$  is fine in  $\Gamma$ , then  $Mi \rightarrow M'i$  is fine in  $\Gamma$ .
- (vii) If  $M \rightarrow M'$  is fine in  $\Gamma$ , then  $\Lambda X.M \rightarrow \Lambda X.M'$  is fine in  $\Gamma$ .
- (viii) If  $M \rightarrow M'$  is fine in  $\Gamma$ , then  $MB \rightarrow M'B$  is fine in  $\Gamma$ .

If  $(M, M', \Gamma) \in \mathcal{R}$ , we write “ $M R M'$  is fine in  $\Gamma$ ”. We now want to define the “compatible closure” of  $\mathcal{R}$ , that will be written “ $M \rightarrow_R M'$  is fine in  $\Gamma$ ”: it is another ternary relation defined inductively by closing  $\mathcal{R}$  under the closure rules in Fig. 7.

5.  $M$  is a fine  $\varrho\rho$ -normal form in  $\Gamma$  if  $M \rightarrow_{\varrho\rho} M'$  is fine in  $\Gamma$  for no  $M'$ .

6. The closures

- “ $M \rightarrow_R^+ M'$  is fine in  $\Gamma$ ”,
- “ $M \rightarrow_R^* M'$  is fine in  $\Gamma$ ” (fine  $R$ -reduction in  $\Gamma$ ),
- “ $M =_R M'$  is fine in  $\Gamma$ ” (fine  $R$ -equality in  $\Gamma$ ),

of “ $M \rightarrow_R M'$  is fine in  $\Gamma$ ” are obtained by closing the latter under the appropriate closure rules from the following list:

- (a)  $M \rightarrow M$  is fine in  $\Gamma$  (fine reflexivity).
- (b) If  $M \rightarrow M'$  is fine in  $\Gamma$ , then  $M' \rightarrow M$  is fine in  $\Gamma$  (fine symmetry).
- (c) If  $M \rightarrow M'$  is fine in  $\Gamma$  and  $M' \rightarrow M''$  is fine in  $\Gamma$ , then  $M \rightarrow M''$  is fine in  $\Gamma$  (fine transitivity).

If we erase the  $\Gamma$ ’s from the rules in Fig. 7, then we obtain the ordinary closure rules defining the compatible closure. Therefore, if  $M \rightarrow_R M'$  is fine in  $\Gamma$ , then  $M \rightarrow_R M'$ . In addition, we know that the  $R$ -redex contracted in this reduction step is fine in some  $\Gamma'$  containing  $\Gamma$  (the extra declarations in  $\Gamma'$  are those relative to the  $\lambda$ -abstractions crossed when going from the root of  $M$  to the root of the contracted redex).

**Proposition 4** (Fine subject reduction). *If  $M \rightarrow_{\varrho\rho} M'$  is fine in  $\Gamma$  and  $M$  has type  $A$  in  $\Gamma$ , then  $M'$  has type  $A$  in  $\Gamma$ .*

*Proof.* By induction on  $M \rightarrow_{\rho\rho} M'$  fine in  $\Gamma$ . For the base cases, going through the  $\rho$ -rules, we check that, if a  $\rho$ -redex  $MC\langle\lambda x^A.P, \lambda y^B.Q\rangle$  is fine and has a type in  $\Gamma$ , then that type is  $C$ , and  $C$  is also the type of its contractum. Similarly for the  $\rho$ -rules. The inductive cases are routine.  $\square$

**Proposition 5** (Fine termination). *Fine  $\rho\rho$ -reduction in  $\Gamma$  starting from a typable term in  $\Gamma$  is terminating.*

*Proof.* First, given a type  $C$ , its size  $|C|$  is defined by:  $|X| = 0$ ;  $|A \supset B| = 2|B|^2 + 3|B| + 1$ ;  $|A \wedge B| = 1 + |A| + |B|$ ;  $|\forall X.A| = 1 + |A|$ .

Next, we define a *pre-redex* to be a term of the forms  $MCQ$  or  $MC$ , where  $C$  is not atomic. In the first case, the pre-redex is a generalization of a  $\rho$ -redex; and in the second case the pre-redex is exactly a  $\rho$ -redex. Pre-redexes are ranged over by  $r$ . We say a pre-redex  $MCQ$  is *fine in  $\Gamma$*  if, for some types  $A$  and  $B$ ,  $M$  has type  $A \vee B$  in  $\Gamma$ ; and say the pre-redex  $MC$  is *fine in  $\Gamma$*  if  $M$  has type  $\perp$  in  $\Gamma$ . If the pre-redex  $MCQ$  is fine in  $\Gamma$ ,  $MC$  is *not* another pre-redex fine in  $\Gamma$  (because the type of  $M$  in  $\Gamma$  is not  $\perp$ ).

Given  $M$  typable in  $\Gamma$  with type  $A$ , say, and given an occurrence of a subterm  $N$  of  $M$ , this occurrence, together with the unique typing derivation of  $\Gamma \vdash M : A$  determine a  $\Gamma'$  such that  $N$  is typable in  $\Gamma'$ : such an occurrence is called a *pre-redex occurrence in  $M$  (according to  $\Gamma$ )* if  $N$  is a pre-redex fine in the determined  $\Gamma'$ . Each pre-redex occurrence in  $M$  is thus the occurrence of some pre-redex  $r$  and has an associated environment  $\Gamma'$ . Different pre-redex occurrences in  $M$  will be denoted  $r_1, r_2$ , etc. When we write  $r_i$ , we mean an occurrence of pre-redex  $r$ , and the related environment is denoted  $\Gamma^{r_i}$ . Let  $\mathcal{R}$  be the set of pre-redex occurrences in  $M$ . Define

$$W(M; \Gamma) := \sum_{r_i \in \mathcal{R}} w(r; \Gamma^{r_i}) ,$$

where  $w(r; \Gamma')$  is defined as follows:

- if  $r = PCQ$ , then  $w(r; \Gamma') = |C|(1 + W(P; \Gamma') + W(Q; \Gamma'))$ ;
- if  $r = PC$ , then  $w(r; \Gamma') = |C|(1 + W(P; \Gamma'))$ .

Now suppose  $M$  is itself a pre-redex  $r$  fine in  $\Gamma$ . Let us calculate  $W(r; \Gamma)$ :

- if  $r = PCQ$ , then  $W(r; \Gamma) = w(r; \Gamma) + W(P; \Gamma) + W(Q; \Gamma)$ , hence

$$W(r; \Gamma) = (|C| + 1)(W(P; \Gamma) + W(Q; \Gamma)) + |C| \quad (*)$$

- if  $r = PC$ , then  $W(r; \Gamma) = w(r; \Gamma) + W(P; \Gamma)$ , hence

$$W(r; \Gamma) = (|C| + 1)(W(P; \Gamma)) + |C| \quad (**)$$

Notice how, in these calculations, we do not make use of the concrete definition of  $|C|$ . The same is true of the recursive definition of  $W$  we give next, which relies on the previous calculations.

The easy cases read:

$$\begin{aligned}
W(x; \Gamma) &= 0 \\
W(\lambda x^A.M; \Gamma) &= W(M; \Gamma, x : A) \\
W(\langle M_1, M_2 \rangle; \Gamma) &= W(M_1; \Gamma) + W(M_2; \Gamma) \\
W(Mi; \Gamma) &= W(M; \Gamma) \\
W(\Lambda X.M; \Gamma) &= W(M; \Gamma)
\end{aligned}$$

As to  $W(MC; \Gamma)$ : if  $MC$  is not a pre-redex fine in  $\Gamma$ , then  $W(MC; \Gamma) = W(M; \Gamma)$ ; otherwise,  $W(MC; \Gamma) = (|C| + 1)W(M; \Gamma) + |C|$ , due to  $(**)$  above. Notice that, when  $C$  is atomic (hence  $MC$  is not a pre-redex and  $|C| = 0$ ),  $(|C| + 1)W(M; \Gamma) + |C| = W(M; \Gamma)$ , so it does not matter which branch of the definition we use to calculate.

As to  $W(MN; \Gamma)$ : if  $MN$  is not a pre-redex fine in  $\Gamma$ , then  $W(MN; \Gamma) = W(M; \Gamma) + W(N; \Gamma)$ ; otherwise  $MN = PCN$ ,  $M = PC$  is not a pre-redex fine in  $\Gamma$  (because the type of  $P$  in  $\Gamma$  is not  $\perp$ ), hence  $W(M; \Gamma) = W(P; \Gamma)$ , and therefore  $W(MN; \Gamma) = (|C| + 1)(W(M; \Gamma) + W(N; \Gamma)) + |C|$ , due to  $(*)$  above. Notice that, when  $M = PC$  with  $C$  atomic (hence  $MN = PCN$  is not a pre-redex and  $|C| = 0$ ), it does not matter again which branch of the definition we use to calculate, because  $(|C| + 1)(W(M; \Gamma) + W(N; \Gamma)) + |C| = W(M; \Gamma) + W(N; \Gamma)$ .

All is in place to prove:

$$\text{If } M \rightarrow_{\varrho\rho} N \text{ is fine in } \Gamma, \text{ then } W(M; \Gamma) > W(N; \Gamma). \quad (***)$$

If  $M$  is typable in  $\Gamma$ , termination of fine  $\varrho\rho$ -reduction in  $\Gamma$  starting from  $M$  follows from  $(***)$  and the fact that  $N$  is also typable in  $\Gamma$  (due to fine subject reduction).

The proof of  $(***)$  is by induction on  $M \rightarrow_{\varrho\rho} N$  fine in  $\Gamma$ , and we will make use of the recursive definition of  $W$ .

For the base cases, we have to check each conversion rule in Def. 4. The rules when  $C = C_1 \wedge C_2$  are challenging, because they cause duplication of terms. But, since measure  $W$  is weighting pre-redexes, the  $\varrho$ -rule when  $C = C_1 \supset C_2$  is challenging as well, since it generates new pre-redexes in some cases. The concrete definition of  $|C|$  is important in proving the base cases.

Case  $LHS := M(C_1 \supset C_2)\langle \lambda x^A.P, \lambda y^B.Q \rangle \rightarrow_{\varrho} \lambda z^{C_1} MC_2\langle \lambda x^A.Pz, \lambda y^B.Qz \rangle =: RHS$ . Since  $z \notin FV(M)$ ,  $W(M; \Gamma, z : C_1) = W(M; \Gamma)$ , so we just write  $W(M)$ . Similarly for  $P$  and  $Q$ . The most favorable case, the case when  $W(RHS)$  is smaller, is when neither  $Pz$  nor  $Qz$  is a new pre-redex. Then,  $W(Pz) = W(P)$  and  $W(Qz) = W(Q)$ , and we calculate:

$$\begin{aligned}
&W(LHS) \\
&= (|C_1 \supset C_2| + 1)(W(M) + W(P) + W(Q)) + |C_1 \supset C_2| \\
&\geq (|C_2| + 1)(W(M) + W(P) + W(Q)) + |C_1 \supset C_2| \\
&> (|C_2| + 1)(W(M) + W(P) + W(Q)) + |C_2| \\
&= (|C_2| + 1)(W(M) + W(Pz) + W(Qz)) + |C_2| \\
&= W(RHS)
\end{aligned}$$

We jump immediately to the less favorable case, when both  $Pz$  and  $Qz$  are pre-redexes. This means that  $P = P'C_2$ ,  $Q = Q'C_2$ ,  $P'$  and  $Q'$  have type  $A' \vee B'$ , and  $C_1 = (A' \supset$

$C_2) \wedge (B' \supset C_2)$ , for some  $P', Q', A'$  and  $B'$ . In this case,  $W(P) = W(P'), W(Q) = W(Q'), W(Pz) = (|C_2| + 1)W(P') + |C_2|$  and  $W(Qz) = (|C_2| + 1)W(Q') + |C_2|$ . Then

$$\begin{aligned}
& W(RHS) \\
&= (|C_2| + 1)(W(M) + W(Pz) + W(Qz)) + |C_2| \\
&= (|C_2| + 1)W(M) + (|C_2| + 1)^2W(P') + (|C_2| + 1)^2W(Q') + 2|C_2|^2 + 3|C_2| \\
&\leq (|C_2| + 1)^2(W(M) + W(P') + W(Q')) + 2|C_2|^2 + 3|C_2| \\
&\leq (|C_1 \supset C_2| + 1)(W(M) + W(P') + W(Q')) + 2|C_2|^2 + 3|C_2| \\
&= (|C_1 \supset C_2| + 1)(W(M) + W(P) + W(Q)) + 2|C_2|^2 + 3|C_2| \\
&< (|C_1 \supset C_2| + 1)(W(M) + W(P) + W(Q)) + 2|C_2|^2 + 3|C_2| + 1 \\
&= (|C_1 \supset C_2| + 1)(W(M) + W(P) + W(Q)) + |C_1 \supset C_2| \\
&= W(LHS)
\end{aligned}$$

Case  $LHS := M(C_1 \wedge C_2) \langle \lambda x^A.P, \lambda y^B.Q \rangle \rightarrow_{\varrho} \langle MC_i \langle \lambda x^A.Pi, \lambda y^B.Qi \rangle \rangle_{i=1,2} =: RHS$ . We calculate, omitting the fixed argument  $\Gamma$  of  $W$ :

$$\begin{aligned}
& W(LHS) \\
&= (|C_1| + |C_2| + 2)(W(M) + W(P) + W(Q)) + |C_1| + |C_2| + 1 \\
&= (|C_1| + 1)(W(M) + W(P) + W(Q)) + |C_1| + \\
&\quad + (|C_2| + 1)(W(M) + W(P) + W(Q)) + |C_2| + 1 \\
&= W(MC_1 \langle \lambda x^A.P1, \lambda y^B.Q1 \rangle) + W(MC_2 \langle \lambda x^A.P2, \lambda y^B.Q2 \rangle) + 1 \\
&= W(RHS) + 1
\end{aligned}$$

Case  $LHS := M(C_1 \wedge C_2) \rightarrow_{\rho} \langle MC_i \rangle_{i=1,2} =: RHS$ . We calculate:

$$\begin{aligned}
& W(LHS) \\
&= (|C_1| + |C_2| + 2)W(M) + |C_1| + |C_2| + 1 \\
&= (|C_1| + 1)W(M) + |C_1| + (|C_2| + 1)W(M) + |C_2| + 1 \\
&= W(MC_1) + W(MC_2) + 1 \\
&= W(RHS) + 1
\end{aligned}$$

Case  $M = \lambda x^A.M' \rightarrow_{\varrho\rho} \lambda x^A.N' = N$ , with  $M' \rightarrow_{\varrho\rho} N'$  fine in  $\Gamma, x : A$ . By IH,  $W(M'; \Gamma, x : A) > W(N'; \Gamma, x : A)$ . Hence  $W(M; \Gamma) > W(N; \Gamma)$ , because  $W(M; \Gamma) = W(M'; \Gamma, x : A)$  and  $W(N; \Gamma) = W(N'; \Gamma, x : A)$ .

Equally easy are: the case  $M = \Lambda X.M' \rightarrow_{\varrho\rho} \Lambda X.N' = N$ , with  $M' \rightarrow_{\varrho\rho} N'$  fine in  $\Gamma$ ; the case  $M = \langle M_1, M_2 \rangle \rightarrow_{\varrho\rho} \langle N_1, M_2 \rangle = N$ , with  $M_1 \rightarrow_{\varrho\rho} N_1$  fine in  $\Gamma$ ; the case  $M = \langle M_1, M_2 \rangle \rightarrow_{\varrho\rho} \langle M_1, N_2 \rangle = N$ , with  $M_2 \rightarrow_{\varrho\rho} N_2$  fine in  $\Gamma$ ; and the case  $M = M'i \rightarrow_{\varrho\rho} N'i = N$ , with  $M' \rightarrow_{\varrho\rho} N'$  fine in  $\Gamma$ . They all follow by IH and application of the recursive definition of  $W$ .

Case  $M = M_1M_2 \rightarrow_{\varrho\rho} N_1M_2 = N$  with  $M_1 \rightarrow_{\varrho\rho} N_1$  fine in  $\Gamma$ . By IH,  $W(M_1; \Gamma) > W(N_1; \Gamma)$ . First, we prove this important remark:  $M$  is a pre-redex fine in  $\Gamma$  iff  $N$  is a pre-redex fine in  $\Gamma$ . The “only if” implication is easy to see. The “if” implication is slightly more involved: if  $N$  is a pre-redex, then  $N_1 = N'_1C$ , for some  $N'_1, C$ , and the circumstance  $M_1 \rightarrow_{\varrho\rho} N_1$  implies that  $M_1 = M'_1C$  and  $M'_1 \rightarrow_{\varrho\rho} N'_1$ , since no root  $\varrho\rho$ -reduction can produce the instantiation  $N'_1C$ . Both implications use fine subject reduction. Now that the remark is proved, we continue:

- First sub-case:  $M$  is a pre-redex. Then  $N$  is a pre-redex,  $W(M; \Gamma) = (|C| + 1)(W(M_1; \Gamma) + W(M_2; \Gamma)) + |C|$ , and  $W(N; \Gamma) = (|C| + 1)(W(N_1; \Gamma) + W(M_2; \Gamma)) + |C|$ . So  $W(M; \Gamma) > W(N; \Gamma)$  follows from  $W(M_1; \Gamma) > W(N_1; \Gamma)$ .
- Second sub-case:  $M$  is not a pre-redex. Then  $N$  is not a pre-redex,  $W(M; \Gamma) = W(M_1; \Gamma) + W(M_2; \Gamma)$ , and  $W(N; \Gamma) = W(N_1; \Gamma) + W(M_2; \Gamma)$ . So  $W(M; \Gamma) > W(N; \Gamma)$  follows again from  $W(M_1; \Gamma) > W(N_1; \Gamma)$ .

The remaining two cases are proved similarly, each with the help of an “important remark”, saying that  $M$  is a pre-redex fine in  $\Gamma$  iff  $N$  is a pre-redex fine in  $\Gamma$ , and very easy to prove, using fine subject reduction. There is the case of  $M = M_1 M_2 \rightarrow_{\varrho\rho} M_1 N_2 = N$  with  $M_2 \rightarrow_{\varrho\rho} N_2$  fine in  $\Gamma$ : its proof finished off very similarly to the previous case, by IH, the important remark and the recursive definition of  $W$ . The last case is  $M = M' C \rightarrow_{\varrho\rho} N' C = N$  with  $M' \rightarrow_{\varrho\rho} N'$  fine in  $\Gamma$ : its proof is finished off in the same way.  $\square$

**Proposition 6** (Atomic normal form). *If  $M$  is typable in  $\Gamma$ , then  $M$  has a unique fine  $\varrho\rho$ -normal form in  $\Gamma$  (which we call the atomic normal form of  $M$  in  $\Gamma$ ).*

*Proof.* Fine termination guarantees the existence of normal forms. As to uniqueness, we need to prove that fine  $\varrho\rho$ -reduction in  $\Gamma$  is confluent. By Newman’s Lemma [12], it suffices to show local confluence. Suppose that  $M \rightarrow_{\varrho\rho} N_1$  and  $M \rightarrow_{\varrho\rho} N_2$  are fine in  $\Gamma$ . The two redexes contracted in these two steps can only overlap trivially (otherwise, in some  $\Gamma'$ , some  $M' C$  would be a fine  $\rho$ -redex and, at the same time, part of a fine  $\varrho$ -redex  $M' C Q$ , and hence  $M'$  would have two different types in  $\Gamma'$ ); but then it is easy to joint  $N_1$  and  $N_2$  in a common  $\varrho\rho$ -reduct.  $\square$

This concludes the investigation of typable atomization. We turn briefly to  $\delta$  and commutative conversions. The problem with subject reduction observed in the beginning of this subsection with  $\varrho$  is observed again with the  $\delta$ -rules in Def. 5 and the  $\varepsilon$ -rules (resp.  $\epsilon$ -rules) in Def. 6. If we are given  $\Gamma$  where the redex is typable, the corresponding contractum is typable only if, additionally,  $M$  has type  $A \downarrow B$  (resp. type  $\perp$ ) in  $\Gamma$ . This determines what it means to be a  $\delta$ -,  $\varepsilon$ - or  $\epsilon$ -redex fine in  $\Gamma$ , and therefore what it means, for a root  $\delta$ -,  $\varepsilon$ - or  $\epsilon$ -reduction, to be fine in  $\Gamma$ .

A root  $\beta\eta$ -reduction is always fine in  $\Gamma$ . Hence, given  $R$  any combination of  $\beta, \eta, \delta, \varepsilon, \epsilon, \varrho, \rho$ , we know what it means to be a root  $R$ -reduction fine in  $\Gamma$ . Following the path in Def. 7, we define the versions of  $\rightarrow_R, \rightarrow_R^+, \rightarrow_R^*$  and  $=_R$  fine in  $\Gamma$ .

Now we have the tools to answer the question at the end of Subsection 4.2, by providing an addendum to the strict simulation theorem.

**Theorem 1 (full version):** *If  $M_1 \rightarrow M_2$  in IPC, then  $M_1^\bullet \rightarrow_{\beta\eta\varepsilon\delta}^+ M_2^\bullet$  and  $M_1^\bullet \rightarrow_{\beta\eta\varrho\rho}^+ M_2^\bullet$  in  $\mathbf{F}$ ; moreover, these reductions are fine in  $\Gamma^\bullet$ , if  $M_1$  is typable in  $\Gamma$ .*

*Proof.* We have to go through all the cases in the proof of Theorem 1 and check the extra statement. Let us start with the base cases. Again, reduction rules that just generate  $\beta\eta$ -steps in the target are no trouble, since  $\beta\eta$ -reduction is always fine in any environment. So we have to check rule  $\eta_\vee$ , the various  $\pi$ -rules, and the various  $\varpi$ -rules.

From the assumption that the redex is typable in  $\Gamma$ , a term  $M$  has type  $A \vee B$  or  $\perp$  as expected, and so  $M^\bullet$  has type  $A^\bullet \vee B^\bullet$  or  $\perp$  as required to make all the  $\delta$ ,  $\varepsilon$  or  $\epsilon$ -steps in the shown simulation be fine in  $\Gamma^\bullet$ . As to the inductive cases, they become routine, as soon as we realize that, for  $S \in \{\beta, \eta, \varepsilon, \epsilon, \eta\delta\}$ , the relations “ $N \rightarrow_S N'$  is fine in  $\Delta$ ” and “ $N \rightarrow_S^+ N'$  is fine in  $\Delta$ ” not only enjoy the fine closure rules of Fig. 7, but also another set of rules, the derivable rules that are the fine versions of those in Fig. 5, and which we refrain to write down.  $\square$

In a similar way we can go again through the proof of Prop. 3, to conclude, in particular: if  $M \rightarrow_{\varrho\rho} N$  is fine in  $\Gamma$ , then  $M =_{\varepsilon\epsilon\eta} N$  is fine in  $\Gamma$ . We note a further consequence, to be used in the next subsection:

$$\text{If } M =_{\varrho\rho} N \text{ is fine in } \Gamma, \text{ then } M =_{\varepsilon\epsilon\eta} N \text{ is fine in } \Gamma. \quad (5)$$

We finish this subsection with a final comments on  $\varepsilon$  and  $\epsilon$ . Consider again rule  $\varepsilon'$

$$\mathcal{E}[\underline{\text{CASE}}(M, x^A.P, y^B.Q, C)] \rightarrow \underline{\text{CASE}}(M, x^A.\mathcal{E}[P], y^B.\mathcal{E}[Q], D) ,$$

and say this root reduction is *fine in*  $\Gamma$  if  $M$  has type  $A \vee B$  in  $\Gamma$  and, furthermore,  $\mathcal{E}$  has type  $D$  and hole of type  $C$  in  $\Gamma$ . Then, the connections between  $C$  and  $D$ , spelled out in (4), are guaranteed by the typing rules for elimination contexts. So, such root reduction, when fine in  $\Gamma$ , is a root  $\varepsilon$ -reduction fine in  $\Gamma$ . The inverse is not necessarily true: in the case of  $\mathcal{E} = [\_ ]N$ , the typing rules give the bonus of  $N$  typable in  $\Gamma$ , which is not necessarily the case in a fine root  $\varepsilon$ -reduction. The perfect match is obtained when the redex is typable: if  $M$  is typable in  $\Gamma$ , then  $M \rightarrow N$  is a fine root  $\varepsilon$ -reduction in  $\Gamma$  iff  $M \rightarrow N$  is a fine root  $\varepsilon'$ -reduction in  $\Gamma$ . Expressing  $\varepsilon$  as the single rule  $\varepsilon'$  will be used in the next subsection.

Similarly for root  $\epsilon$ -reduction and the  $\epsilon'$ -rule  $\mathcal{E}[\underline{\text{ABORT}}(M, C)] \rightarrow \underline{\text{ABORT}}(M, D)$ .

#### 4.4 Connection with dinaturality conversions

In this subsection we prove that adding fine atomization conversions to system **F** does not cause the system to become inconsistent. In view of (5), it suffices to show the same for the addition of commutative conversions  $\varepsilon$  and  $\epsilon$ . The strategy of the proof is the one that is implicit in [11] in the informal justification that some general form of commutative conversions does not break consistency: one shows that the equality generated by adding the commutative conversions is contained in a bigger equality which is known to be consistent. Here, for the latter, we take the equality obtained by adding to system **F** a *dinaturality conversion*, which we denote  $\nu$ .

The full formalization of  $\nu$  would require bringing here the machinery of [8]. We refrain from doing that and just give a brief indication. Given formulas  $A, C^+, C^-$  and a type variable  $X$ , the formula that results from substituting  $C^+$  (resp.  $C^-$ ) for the positive (resp. negative) occurrences of  $X$  in  $A$  is denoted  $[(C^-, C^+)/X]A$ . Notice  $[(C, C)/X]A = [C/X]A$ . Let  $\mathcal{F}$  be the free category generated from system **F** (the “syntactic” category) by the usual method of categorical logic. Then, each  $A$  determines a functor  $[(\_, \_)/X]A : \mathcal{F}^{op} \times \mathcal{F} \rightarrow \mathcal{F}$ . We refer the reader to [8] for the definition  $[(f^-, f^+)/X]A$ , for morphism  $f^-, f^+$ .

Let  $x : A_1 \vdash t : A_2$ . The family of morphisms  $[C/X]t : [(C, C)/X]A_1 \rightarrow [(C, C)/X]A_2$  over  $C$  is a *dinatural transformation* between the functors  $[(-, -)/X]A_1$  and  $[(-, -)/X]A_2$  if, for every morphism  $u : C \rightarrow D$ , a certain diagram commutes, which means that certain two terms, determined by the given data, namely

$$[(u, 1_C)/X]A_1; [C/X]t; [(1_C, u)/X]A_2$$

and

$$[(1_D, u)/X]A_1; [D/X]t; [(u, 1_D)/X]A_2 \quad ,$$

are  $\beta\eta$ -equal in system **F**. In [8] a characterization is given of the terms  $t$  which determine dinatural transformations. Conversion  $\nu$  states that the referred diagram always commutes, that is, the above two terms are always equal. Hence, in system **F** plus  $\nu$ , every typable term determines a dinatural transformation.

We now show that  $\varepsilon' \subseteq_{\beta\eta\nu}$  (more precisely, a root  $\varepsilon'$ -reduction step fine in  $\Gamma$  is contained in  $=_{\beta\eta\nu}$ ). Let  $M$  be such that  $\Gamma \vdash M : A \downarrow B$ . Let  $X$  be a type variable not free in  $M$ , and  $P, P'$  be of type  $C$ , and  $\Gamma|C \vdash \mathcal{E} : D$ . For the purpose of matching the following calculation with the notation in the previous paragraphs, it is useful to put  $t := MX\langle x, x' \rangle$ . Then  $\Gamma, x : A \supset X, x' : B \supset X \vdash t : X$ , so we may put  $A_1 := (A \supset X) \wedge (B \supset X)$  and  $A_2 := X$ . Then:

$$\begin{aligned} \mathcal{E}[MC\langle \lambda z^A.P, \lambda z'^B.P' \rangle] &=_{\eta} \mathcal{E}[MC\langle \lambda y.(\lambda z^A.P)y, \lambda y'.(\lambda z'^B.P')y' \rangle] \\ &= [\lambda z.P/x][\lambda z'.P'/x'](\mathcal{E}[MC\langle \lambda y.xy, \lambda y'.x'y' \rangle]) \\ &=_{\nu} [\lambda z.P/x][\lambda z'.P'/x'](MC\langle \lambda y.\mathcal{E}[xy], \lambda y'.\mathcal{E}[x'y'] \rangle) \\ &= MC\langle \lambda y.\mathcal{E}[(\lambda z.P)y], \lambda y'.\mathcal{E}[(\lambda z'.P')y'] \rangle \\ &=_{\beta} MC\langle \lambda y.\mathcal{E}[[y/z]P], \lambda y'.\mathcal{E}[[y'/z']P'] \rangle \\ &= MC\langle \lambda z.\mathcal{E}[P], \lambda z'.\mathcal{E}[P'] \rangle \end{aligned}$$

The  $\nu$ -conversion in this calculation is justified as follows. Before the conversion, we find the term  $MC\langle \lambda y.xy, \lambda y'.x'y' \rangle$ , which is  $[N/x][N'/x'] [C/X]t$ , where  $N = \lambda y.xy$  is  $[(\mathcal{E}, 1_C)/X](A \supset X)$  and  $N' = \lambda y'.x'y'$  is  $[(\mathcal{E}, 1_C)/X](B \supset X)$ . Since  $A_2 = X$ ,  $[(1_C, \mathcal{E})/X]A_2 = \mathcal{E}$ . After the conversion, notice that  $\lambda y.\mathcal{E}[xy]$  is  $[(1_D, \mathcal{E})/X](A \supset X)$  and  $\lambda y'.\mathcal{E}[x'y']$  is  $[(1_D, \mathcal{E})/X](B \supset X)$ . Since  $A_2 = X$ ,  $[(u, 1_D)/X]A_2 = 1_D$ .

As to  $\varepsilon$ , it turns out that  $\varepsilon' \subseteq_{\nu} \varepsilon$ . Let  $M$  be such that  $\Gamma \vdash M : \perp$ . Let  $X$  be a type variable not free in  $M$ , and  $C \vdash \mathcal{E} : D$ . For the purpose of recognizing a  $\nu$ -conversion, it is useful to put  $t := MX$  and allow a type 1. Then  $\Gamma, x : 1 \vdash t : X$ , so we may put  $A_1 := 1$  and  $A_2 := X$ . From type 1 we just require that  $X$  does not occur in 1, and that  $[(f^-, f^+)/X]1$  is the identity  $1_1$ , that is 1 as a trivial derivation. Then:

$$\mathcal{E}[MC] =_{\nu} MD \quad .$$

Indeed,  $MC = [C/X]t$  and pre-composition with  $[(\mathcal{E}, id_C)/X]1$ , since the latter is an identity; and  $[(1_C, \mathcal{E})/X]A_2 = \mathcal{E}$ , since  $A_2 = X$ . After the conversion,  $MD = [D/X]t$ , and the pre-composition with  $[(id_D, \mathcal{E})/X]1$  has no effect since the latter is an identity; derivation  $\mathcal{E}$  vanishes since  $[(1_D, \mathcal{E})/X]1$  is a trivial derivation; and  $[(u, 1_D)/X]A_2 = 1_D$ , since  $A_2 = X$ .

**Theorem 2** (Consistency). *In system **F** there are terms  $M, N$  typable in  $\Gamma$  such that  $M =_{\beta\eta\eta\rho} N$  is not fine in  $\Gamma$ .*



*Proof.* Having in mind (5) and the calculations above, we conclude: for all  $M, N$  typable in  $\Gamma$ , if  $M =_{\beta\eta\theta\rho} N$  is fine in  $\Gamma$ , then  $M =_{\beta\eta\nu} N$ . To complete the proof, we just invoke the consistency of  $=_{\beta\eta\nu}$ , which guarantees the existence of  $M$  and  $N$  typable in  $\Gamma$  such that  $M =_{\beta\eta\nu} N$  does not hold. The consistency of  $=_{\beta\eta\nu}$ , in turn, follows from the results in [2], where models of system **F** (with product types) are given such that every typable term in **F** is interpreted by a dinatural transformation, hence validating the dinatural conversion  $\nu$ .  $\square$

## 5 Comparison of embeddings

We recall the optimized translation of **IPC** into **F<sub>at</sub>**, introduced by the authors in [3], and denoted  $(\cdot)^\circ$ . It comprises a translation of formulas, which is the same as in the Russell-Prawitz translation, so  $A^\circ = A^\bullet$ ; and comprises a translation of proof-terms (which induces a translation of derivations).

The translation of proof terms will rely on the following definition, taken from [3]:

**Definition 8.** In **F<sub>at</sub>**:

1. Given  $M, A, B$ , given  $i \in \{1, 2\}$ , we define

$$\underline{\text{in}}_i(M, A, B) := \Lambda X. \lambda w^{(A \supset X) \wedge (B \supset X)}. w i M,$$

where the bound variable  $X$  is chosen so that  $X \notin M, A, B$ .

2. Given  $M, P, Q, A, B, C$ , we define  $\underline{\text{case}}(M, x^A.P, y^B.Q, C)$  by recursion on  $C$  as follows:

$$\begin{aligned} \underline{\text{case}}(M, x^A.P, y^B.Q, X) &= M X \langle \lambda x^A.P, \lambda y^B.Q \rangle \\ \underline{\text{case}}(M, x^A.P, y^B.Q, C_1 \wedge C_2) &= \langle \underline{\text{case}}(M, x^A.P, y^B.Q, C_1), \underline{\text{case}}(M, x^A.P, y^B.Q, C_2) \rangle_{i=1,2} \\ \underline{\text{case}}(M, x^A.P, y^B.Q, C \supset D) &= \lambda z^C. \underline{\text{case}}(M, x^A.Pz, y^B.Qz, D) \\ \underline{\text{case}}(M, x^A.P, y^B.Q, \forall X.C) &= \Lambda X. \underline{\text{case}}(M, x^A.PX, y^B.QX, C) \end{aligned}$$

where, in the third clause, the bound variable  $z$  is chosen so that  $z \neq x, z \neq y$  and  $z \notin M, P, Q$ ; and in the fourth clause, the bound variable  $X$  is chosen so that  $X \notin M, P, Q, A, B$ .

3. Given  $M, A$ , we define  $\underline{\text{abort}}(M, A)$  by recursion on  $A$  as follows:

$$\begin{aligned} \underline{\text{abort}}(M, X) &= M X \\ \underline{\text{abort}}(M, A_1 \wedge A_2) &= \langle \underline{\text{abort}}(M, A_1), \underline{\text{abort}}(M, A_2) \rangle \\ \underline{\text{abort}}(M, B \supset C) &= \lambda z^B. \underline{\text{abort}}(M, C) \\ \underline{\text{abort}}(M, \forall X.A) &= \Lambda X. \underline{\text{abort}}(M, A) \end{aligned}$$

where, in the third clause, the bound variable  $z$  is chosen so that  $z \notin M$ ; and in the fourth clause, the bound variable  $X$  is chosen so that  $X \notin M$ .

If we take the typing rules in Fig. 4 and replace **IN**, **CASE**, and **ABORT** by  $\underline{\text{in}}$ ,  $\underline{\text{case}}$ , and  $\underline{\text{abort}}$ , respectively, we obtain admissible typing rules in **F<sub>at</sub>**. Similarly, if we do the same replacements in Fig. 5, we obtain admissible compatibility rules in **F<sub>at</sub>**. Such admissible rules in **F<sub>at</sub>** have been observed in [3].

**Definition 9.** Given  $M \in \mathbf{IPC}$ ,  $M^\circ$  is defined by recursion on  $M$  exactly as in Fig. 6, except for the translation of in, case and abort, which now reads:

$$\begin{aligned} (\text{in}_i(M, A, B))^\circ &= \underline{\text{in}}_i(M^\circ, A^\circ, B^\circ) \quad (i = 1, 2) \\ (\text{case}(M, x^A.P, y^B.Q, C))^\circ &= \underline{\text{case}}(M^\circ, x^{A^\circ}.P^\circ, y^{B^\circ}.Q^\circ, C^\circ) \\ (\text{abort}(M, A))^\circ &= \underline{\text{abort}}(M^\circ, A^\circ) \end{aligned}$$

**Proposition 7** (Type soundness). *If  $\Gamma \vdash M : A$  in  $\mathbf{IPC}$ , then  $\Gamma^\circ \vdash M^\circ : A^\circ$  in  $\mathbf{F}_{\text{at}}$ .*

To compare how the maps  $(\cdot)^\bullet$  and  $(\cdot)^\circ$  translate proof terms amounts to compare IN, CASE, and ABORT, on the one hand, with in, case, and abort, on the other hand. IN <sub>$i$</sub> ( $M, A, B$ ) and in <sub>$i$</sub> ( $M, A, B$ ) are defined in the same way, the repetition is due to stylistic reasons. The other comparisons use atomization conversions.

**Lemma 2.** *In  $\mathbf{F}$ :  $\underline{\text{CASE}}(M, x^A.P, y^B.Q, C) \rightarrow_\rho^* \underline{\text{case}}(M, x^A.P, y^B.Q, C)$ ; additionally, this reduction is fine in  $\Gamma$ , if  $M$  has type  $A \vee B$  in  $\Gamma$ .*

*Proof.* The proof is by induction on  $C$ . We first check the first statement.

Case  $C = X$ . We calculate:  $LHS = MX\langle\lambda x^A.P, \lambda y^B.Q\rangle = RHS$ , using twice the definition of CASE.

Case  $C = C_1 \supset C_2$ .

$$\begin{aligned} LHS &= M(C_1 \supset C_2)\langle\lambda x^A.P, \lambda y^B.Q\rangle && \text{(by def. of } \underline{\text{CASE}}) \\ &\rightarrow_\rho \lambda z^{C_1}. MC_2\langle\lambda x^A.Pz, \lambda y^B.Qz\rangle \\ &= \lambda z^{C_1}. \underline{\text{CASE}}(M, x^A.Pz, y^B.Qz, C_2) \\ &\rightarrow_\rho^* \lambda z^{C_1}. \underline{\text{case}}(M, x^A.Pz, y^B.Qz, C_2) && \text{(by IH)} \\ &= RHS && \text{(by def. of } \underline{\text{case}}) \end{aligned}$$

Case  $C = C_1 \wedge C_2$ .

$$\begin{aligned} LHS &= M(C_1 \wedge C_2)\langle\lambda x^A.P, \lambda y^B.Q\rangle && \text{(by def. of } \underline{\text{CASE}}) \\ &\rightarrow_\rho \langle MC_i\langle\lambda x^A.Pi, \lambda y^B.Qi\rangle \rangle_{i=1,2} \\ &= \langle \underline{\text{CASE}}(M, x^A.Pi, y^B.Qi, C_i) \rangle_{i=1,2} \\ &\rightarrow_\rho^* \langle \underline{\text{case}}(M, x^A.Pi, y^B.Qi, C_i) \rangle_{i=1,2} && \text{(by IH)} \\ &= RHS && \text{(by def. of } \underline{\text{case}}) \end{aligned}$$

Case  $C = \forall X.C_0$ .

$$\begin{aligned} LHS &= M(\forall X.C_0)\langle\lambda x^A.P, \lambda y^B.Q\rangle && \text{(by def. of } \underline{\text{CASE}}) \\ &\rightarrow_\rho \Lambda X. MC_0\langle\lambda x^A.PX, \lambda y^B.QX\rangle \\ &= \Lambda X. \underline{\text{CASE}}(M, x^A.PX, y^B.QX, C_0) \\ &\rightarrow_\rho^* \Lambda X. \underline{\text{case}}(M, x^A.PX, y^B.QX, C_0) && \text{(by IH)} \\ &= RHS && \text{(by def. of } \underline{\text{case}}) \end{aligned}$$

Now the additional statement. In the case  $C = X$ , there is nothing to check (by definition of fine reflexivity,  $LHS \rightarrow_\rho^* LHS$  in any  $\Gamma$ ).

Case  $C = C_1 \supset C_2$ . If  $M$  has type  $A \vee B$  in  $\Gamma$ , the first  $\rho$ -reduction step in the calculation is, by definition, a fine root step in  $\Gamma$ . Given that  $z \notin M$ ,  $M$  has type  $A \vee B$  in  $\Delta := \Gamma, z : C_1$ . By IH, the reduction under  $\lambda z$  is fine in  $\Delta$ . Given that the relation “ $N \rightarrow_\rho^* N'$  is fine in  $\Delta$ ” enjoys the fine closure rules of Fig. 7, we conclude that the second reduction in the calculation is fine in  $\Gamma$ .

The remaining cases are similar to, but simpler than this one.  $\square$

**Lemma 3.** In  $\mathbf{F}$ ,  $\text{ABORT}(M, C) \rightarrow_{\rho}^* \text{abort}(M, C)$ ; additionally, this reduction is fine in  $\Gamma$ , if  $M$  has type  $\perp$  in  $\Gamma$ .

*Proof.* The proof is by induction on  $C$ . We check first the first statement.

Case  $C = X$ . Then  $LHS = MX = RHS$ , using twice the definition of ABORT.

Case  $C = C_1 \supset C_2$ .

$$\begin{aligned}
 LHS &= M(C_1 \supset C_2) && \text{(by def. of } \underline{\text{ABORT}}) \\
 &\rightarrow_{\rho} \lambda z^{C_1}. MC_2 \\
 &= \lambda z^{C_1}. \text{ABORT}(M, C_2) \\
 &\rightarrow_{\rho}^* \lambda z^{C_1}. \text{abort}(M, C_2) && \text{(by IH)} \\
 &= RHS && \text{(by def. of } \underline{\text{abort}})
 \end{aligned}$$

Case  $C = C_1 \wedge C_2$ .

$$\begin{aligned}
 LHS &= M(C_1 \wedge C_2) && \text{(by def. of } \underline{\text{ABORT}}) \\
 &\rightarrow_{\rho} \langle MC_1, MC_2 \rangle \\
 &= \langle \text{ABORT}(M, C_1), \text{ABORT}(M, C_2) \rangle \\
 &\rightarrow_{\rho}^* \langle \text{abort}(M, C_1), \text{abort}(M, C_2) \rangle && \text{(by IH)} \\
 &= RHS && \text{(by def. of } \underline{\text{abort}})
 \end{aligned}$$

Case  $C = \forall X. C_0$ .

$$\begin{aligned}
 LHS &= M(\forall X. C_0) && \text{(by def. of } \underline{\text{ABORT}}) \\
 &\rightarrow_{\rho} \Lambda X. MC_0 \\
 &= \Lambda X. \text{ABORT}(M, C_0) \\
 &\rightarrow_{\rho}^* \Lambda X. \text{abort}(M, C_0) && \text{(by IH)} \\
 &= RHS && \text{(by def. of } \underline{\text{case}})
 \end{aligned}$$

The justification of the additional statement in each case of the proof is similar to what was done in the proof of the previous lemma.  $\square$

**Proposition 8** (Comparison of maps: proofs). *For all  $M \in \mathbf{IPC}$ ,  $M^{\bullet} \rightarrow_{\rho}^* M^{\circ}$ ; additionally, this relation is fine in  $\Gamma^{\bullet}$ , if  $M$  is typable in  $\Gamma$ . Hence if  $M$  is typable in  $\Gamma$ ,  $M^{\circ}$  is the atomic normal form of  $M^{\bullet}$  in  $\Gamma^{\bullet}$  ( $=\Gamma^{\circ}$ ).*

*Proof.* By induction on  $M$ . There are only two interesting cases, which follow by Lemmas 2 and 3. Notice  $M^{\circ}$  is a fine  $\rho$ -normal form, because  $M^{\circ} \in \mathbf{F}_{\text{at}}$ . Hence, by Proposition 6,  $M^{\circ}$  is the unique  $\rho$ -normal form of  $M^{\bullet}$  in  $\Gamma^{\bullet}$ .  $\square$

We now want to compare how the maps  $(\cdot)^{\bullet}$  and  $(\cdot)^{\circ}$  translate proof-reduction steps. Obviously,  $R$ -reduction steps, with  $R \in \{\beta_{\supset}, \beta_{\wedge}, \eta_{\supset}, \eta_{\wedge}\}$ , are translated in the same way by the two maps. Only the  $R$ -reduction steps, for  $R$  a reduction rule pertaining to  $\vee$  or  $\perp$ , are pertinent for the comparison, and so we concentrate on these from now on. The translation of such steps by  $(\cdot)^{\bullet}$  was detailed in Theorem 1, whereas the translation by  $(\cdot)^{\circ}$  was detailed in [3]. We want to see how the two pictures merge.

Let  $R \in \{\beta_\vee, \pi_\supset, \pi_\wedge, \varpi_\supset, \varpi_\wedge, \varpi_\vee, \varpi_\perp\}$ . A reduction step  $M \rightarrow_R N$  in **IPC** gives rise to the diagram:

$$\begin{array}{ccccc}
 M & & M^\circ & \xleftarrow{\varrho\rho} & M^\bullet \\
 R \downarrow & & \beta\eta \downarrow & & \downarrow \beta\eta\varepsilon\epsilon \\
 N & & N^\circ & \xleftarrow{\varrho\rho} & N^\bullet
 \end{array} \tag{6}$$

This follows from Theorem 1 above, and also from Theorem 1 in [3], which guarantees  $M^\circ \rightarrow_{\beta\eta}^+ N^\circ$ , whenever  $M \rightarrow_R N$  in **IPC**. The  $\varrho\rho$ -reductions that bridges the two translations come from Proposition 8.

This picture has to be generalized, in order to accommodate the remaining cases  $R \in \{\eta_\vee, \pi_\vee, \pi_\perp\}$ . In these cases, the interaction between the terms translated with  $(\cdot)^\bullet$  and those translated with  $(\cdot)^\circ$  will be richer than what can be expressed with Proposition 8. For this reason, we have to revisit Lemmas 6, 11 and 12 in [3], dedicated to  $\eta_\vee$ ,  $\pi_\vee$  and  $\pi_\perp$ , respectively. We do this next, but put the proofs in the appendix, since they are, to some extent, a repetition of the proofs already given in [3].

**Lemma 4** (Rule  $\eta_\vee$ ). *Let  $M \in \mathbf{F}_{\text{at}}$  and  $M' \in \mathbf{F}$  such that  $M' \rightarrow_{\varrho\rho}^* M$ . Let*

$$\begin{aligned}
 LHS &= \underline{\text{case}}(M, x^A.\underline{\text{in}}_1(x, A, B), y^B.\underline{\text{in}}_2(y, A, B), A \vee B) \\
 LHS' &= \underline{\text{CASE}}(M', x^A.\underline{\text{in}}_1(x, A, B), y^B.\underline{\text{in}}_2(y, A, B), A \vee B) \\
 RHS &= M
 \end{aligned}$$

*Then there is  $Q \in \mathbf{F}_{\text{at}}$  such that*

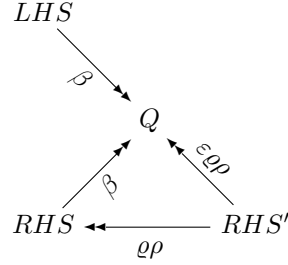
$$\begin{array}{ccc}
 LHS & \xleftarrow{\varrho\rho} & LHS' \\
 \searrow \varrho & & \swarrow \delta\varrho\rho \\
 & Q & \\
 \swarrow \pi & & \\
 RHS & & 
 \end{array}$$

*Proof.* Lemma 6 in [3] just states  $LHS \rightarrow_{\beta\eta}^+ RHS$ . The proof is a direct calculation. See the appendix for details.  $\square$

**Lemma 5** (Rule  $\pi_\vee$ ). *Let  $M, P_1, P_2, Q_1, Q_2 \in \mathbf{F}_{\text{at}}$  and  $M', P'_1, P'_2, Q'_1, Q'_2 \in \mathbf{F}$ . Let*

$$\begin{aligned}
 LHS &= \underline{\text{case}}(\underline{\text{case}}(M, x_1.P_1, x_2.P_2, B_1 \vee B_2), y_1.Q_1, y_2.Q_2, C) \\
 RHS &= \underline{\text{case}}(M, x_1.\underline{\text{case}}(P_1, y_1.Q_1, y_2.Q_2, C), x_2.\underline{\text{case}}(P_2, y_1.Q_1, y_2.Q_2, C), C) \\
 RHS' &= \underline{\text{CASE}}(M', x_1.\underline{\text{CASE}}(P'_1, y_1.Q'_1, y_2.Q'_2, C), x_2.\underline{\text{CASE}}(P'_2, y_1.Q'_1, y_2.Q'_2, C), C)
 \end{aligned}$$

Suppose  $T' \rightarrow_{\epsilon\rho}^* T$ , for  $T = M, P_1, P_2, Q_1, Q_2$ . Then, there is  $Q \in \mathbf{F}_{\text{at}}$  such that



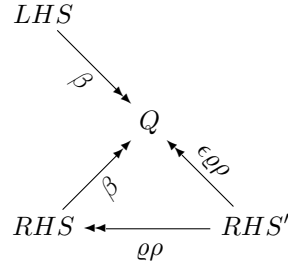
*Proof.* For typographic reasons, we do not write the types of bound variables. Variables  $y_1$  and  $y_2$  have type  $B_1$  and  $B_2$ , respectively. Variables  $x_1$  and  $x_2$  have type  $A_1$  and  $A_2$ , where  $A_1 \vee A_2$  is the type of  $M$ . These types stay unchanged throughout the proof.

Lemma 11 in [3] just states  $LHS =_{\beta} RHS$ . The proof of the present lemma is by induction on  $C$ . See the appendix for details.  $\square$

**Lemma 6** (Rule  $\pi_{\perp}$ ). *Let  $M, P, Q \in \mathbf{F}_{\text{at}}$  and  $M', P', Q' \in \mathbf{F}$ . Let*

$$\begin{aligned} LHS &= \underline{\text{abort}}(\underline{\text{case}}(M, x^A.P, y^B.Q, \perp), C) \\ RHS &= \underline{\text{case}}(M, x^A.\underline{\text{abort}}(P, C), y^B.\underline{\text{abort}}(Q, C), C) \\ RHS' &= \underline{\text{CASE}}(M', x^A.\underline{\text{ABORT}}(P', C), y^B.\underline{\text{ABORT}}(Q', C), C) \end{aligned}$$

Suppose  $T' \rightarrow_{\epsilon\rho}^* T$ , for  $T = M, P, Q$ . Then, there is  $Q \in \mathbf{F}_{\text{at}}$  such that



*Proof.* Lemma 12 in [3] just states  $LHS =_{\beta} RHS$ . The proof is by induction on  $C$ . See the appendix for details.  $\square$

In order to avoid overloading too much the paper, we refrained from stating the full version of Lemmas 4, 5, and 6. But the missing bits say the reduction from  $LHS'$  or  $RHS'$  to  $Q$  is fine in  $\Gamma$ , provided  $M$  has type  $A \vee B$  or  $A_1 \vee A_2$  in  $\Gamma$ , and  $P_1$  has type  $B_1 \vee B_2$  or  $\perp$  in  $\Gamma, x : A_1$  and similarly for  $P_2$ .

For each  $R \in \{\eta_{\vee}, \pi_{\vee}, \pi_{\perp}\}$ , we now show, using Lemmas 4, 5 and 6, a diagram in the style of (6), with a left half in  $\mathbf{IPC}$  and a right half in  $\mathbf{F}$ . For instance, for  $R = \eta_{\vee}$ , the left half is  $M \rightarrow_{\eta_{\vee}} N$  and the right half has the shape of the diagram in the statement of Lemma 4, with  $LHS, RHS$  and  $LHS'$  replaced by  $M^{\circ}, N^{\circ}$  and  $M^{\bullet}$ , respectively. One should complete the diagram by adding  $N^{\bullet}$  (in the place of the missing  $RHS'$ ) and drawing the reductions  $N^{\bullet} \rightarrow_{\epsilon\rho}^* N^{\circ}$  and  $M^{\bullet} \rightarrow_{\eta_{\delta}}^+ N^{\bullet}$  (coming

respectively from Proposition 8 and Theorem 1). We do the same for  $R = \pi_{\vee}$  and  $R = \pi_{\perp}$ , obtaining their respective diagrams.

One last thing. In the diagrams just obtained for  $\eta_{\vee}$ ,  $\pi_{\vee}$ , and  $\pi_{\perp}$ , some reduction steps in the right half are *administrative*, that is, they reduce redexes that do not correspond to redexes in the source terms  $M, N \in \mathbf{IPC}$ , but are redexes that were created by the translation  $(\_)^\circ$  itself. This question was analyzed in detail in [3], specifically how some reduction steps in  $\mathbf{F}_{\text{at}}$  stated by Lemmas 6, 11 and 12 of [3] can be classified as administrative, when they contribute to bridge  $M^\circ$  and  $N^\circ$ . The analysis carries over to reduction steps in  $\mathbf{F}_{\text{at}}$  stated by Lemmas 4, 5 and 6, again when they contribute to bridge  $M^\circ$  and  $N^\circ$  - which is what happens in the diagrams just obtained for  $\eta_{\vee}$ ,  $\pi_{\vee}$ , and  $\pi_{\perp}$ . That analysis allows us to say that: in the diagram for  $\eta_{\vee}$ , the  $\beta$ -reduction steps from  $LHS = M^\circ$  to  $Q$  are administrative; in the diagrams for  $\pi_{\vee}$  and  $\pi_{\perp}$ , the  $\beta$ -reduction steps from  $RHS = N^\circ$  to  $Q$  are administrative.

We now have diagrams in the style of (6) for every reduction rule  $R$  of  $\mathbf{IPC}$  pertaining to disjunction or absurdity. The diagrams for  $\eta_{\vee}$ ,  $\pi_{\vee}$ , and  $\pi_{\perp}$  are slightly more complex, because they have a central term  $Q$ , and some reductions are classified as administrative. But we can define a general pattern that comprehends all of these diagrams, and thus explains the translation of any reduction steps  $M \rightarrow_R N$  in  $\mathbf{IPC}$ :

**Theorem 3** (Comparison of maps: reduction). *For  $M \rightarrow_R N$  in  $\mathbf{IPC}$ , with  $R$  a reduction rule pertaining to disjunction or absurdity, the reductions in Fig. 8 hold. Moreover, if  $M$  is typable in  $\Gamma$ , then all reductions in Fig. 8 starting from  $M^\bullet$  or  $N^\bullet$  are fine in  $\Gamma^\bullet$ .*

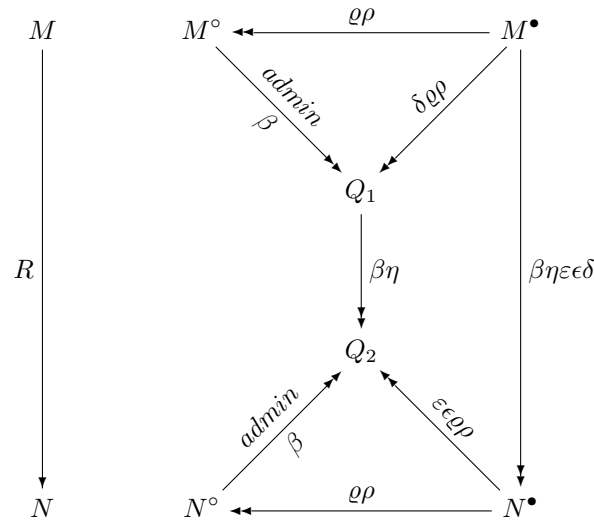
*Proof.* For the second statement, we have to invoke the subject reduction property of  $\rightarrow_R$  in  $\mathbf{IPC}$ , the full version of Theorem 1, Proposition 8, and the full version of Lemmas 4, 5, and 6.  $\square$

## 6 Discussion

We summarize our contribution. We proposed new conversions for system  $\mathbf{F}$  whose purpose is to enforce atomic use of the universal instantiation. Such conversions explain the connection between the Russell-Prawitz translation and the translation into  $\mathbf{F}_{\text{at}}$  introduced by the authors [3], at the level of proofs (Proposition 8) and at the level of proof reduction (Theorem 3). In addition, only when system  $\mathbf{F}$  is thus equipped does the Russell-Prawitz translation preserve proof reduction (Theorem 1) - and this without collapsing proof identity in system  $\mathbf{F}$  (Theorem 2), because the atomization conversions are not stronger than a certain “dinaturality” conversion known to preserve the consistency of equality.

Like the present paper, the recent article [11] aims at finding new conversions for  $\mathbf{NI}^2$  which allow to establish the preservation of proof identity by the Russell-Prawitz translation. In addition to the fact that we employ  $\lambda$ -terms, thereby making explicit the algorithmic aspect of the development, we see three main differences/improvements the present paper offers w.r.t. the work cited. First, we study the Russell-Prawitz

Figure 8: Translation of a  $R$ -reduction step in **IPC**, for  $R$  a reduction rule pertaining to disjunction or absurdity. Terms  $M$  and  $N$  are in **IPC**. Terms  $M^\circ$ ,  $N^\circ$ ,  $Q_1$  and  $Q_2$  are in **F<sub>at</sub>**. Terms  $M^\bullet$  and  $N^\bullet$  are in **F**. If  $M^\circ = Q_1$ , then the reduction  $M^\bullet \rightarrow_{\delta\varrho\rho}^* Q_1$  is actually the reduction  $M^\bullet \rightarrow_{\varrho\rho}^* M^\circ$ . If  $N^\circ = Q_2$ , then the reduction  $N^\bullet \rightarrow_{\varepsilon\varepsilon\varrho\rho}^* Q_2$  is actually the reduction  $N^\bullet \rightarrow_{\varrho\rho}^* N^\circ$ . Notice that, due to Propositions 2 and 3,  $M^\bullet \rightarrow_{\beta\eta\rho\varrho}^* N^\bullet$ .



embedding into  $\mathbf{F}$  side-by-side with another embedding into  $\mathbf{F}_{\text{at}}$ . This comprehensiveness is opportune because the translation into  $\mathbf{F}_{\text{at}}$  was perceived initially [5] as a progress in the matter of preservation of proof identity, our Theorem 3 bringing now a full clarification of the issue. Second, as opposed to the new conversion of [11], expressing “naturality” in the categorical sense, we propose a much simpler new conversion which, despite being connected to a very simple variant of the “naturality” conversion (namely conversions  $\varepsilon$  and  $\epsilon$ ), has a self-contained motivation (atomization of the uses of universal instantiation), and moreover not only delivers preservation of proof identity, but also makes a bridge between the Russell-Prawitz embedding and the embedding into  $\mathbf{F}_{\text{at}}$ . Third, we obtained preservation of proof *reduction* by the Russell-Prawitz embedding, while [11] is only concerned with proof identity.

One wonders whether the results in [11], although stated in terms of proof identity, do establish (or could be modified to establish) results about proof reduction. But, with a single exception (Proposition 4.7. in [11]), the answer is “no”: (i) the results about “m-closed” instances of  $\pi_V$  or  $\eta_V$  rely essentially on an argument (see the proofs of Propositions 2.5 and 2.6 in [11]) that starts with the  $\beta$ -normalization of a  $\pi_V$  or  $\eta_V$  *contractum* - hence this  $\beta$ -normalization goes in the “wrong direction”, does not preserve the direction of reduction; (ii) in the proof of Proposition 4.9 of [11], on preservation of  $\eta_V$ -equality, the Russell-Prawitz translation of the redex starts doing some steps of  $\eta$ -expansion, which again go in the “wrong direction”.

Regarding the various embeddings of  $\mathbf{IPC}$  into system  $\mathbf{F}_{\text{at}}$ , it can be argued that the embedding  $(\_)^\circ$  previously introduced by the authors [3] has advantages over the original embedding based on instantiation overflow [4, 5], in that shorter translations of proofs and of reduction sequences are obtained. In a recent paper in arXiv [9], Pistone, Tranchini and Petrolo independently establish a connection between the Russell-Prawitz translation and yet another translation of  $\mathbf{IPC}$  directly into system  $\mathbf{F}_{\text{at}}$ , showing that they are equivalent modulo an extended equational theory for System  $\mathbf{F}$ . The translation into  $\mathbf{F}_{\text{at}}$  in [9] is not more “economic” than  $(\_)^\circ$ , but the exact comparison between the two deserve further investigation. However, the naturalness of the connection between  $(\_)^\circ$  and the Russell-Prawitz translation established in the present paper, with  $M^\circ$  being the  $\varrho\rho$ -normal form of  $M^\bullet$ , seems to the authors a strong indication of the special place occupied by the embedding  $(\_)^\circ$  into system  $\mathbf{F}_{\text{at}}$ .

Since  $M^\circ$  is the atomic normal form of  $M^\bullet$ , the embedding  $(\_)^\circ$  makes full use of atomization at compile time. But, for the purpose of simulation, what one needs is a judicious use of atomization at run time. As observed in Fig. 8, a reduction from  $M^\circ$  to  $N^\circ$  is still missing, for some cases of reduction  $M \rightarrow N$  in  $\mathbf{IPC}$ , while a reduction always exists between the Russell-Prawitz translations  $M^\bullet$  and  $N^\bullet$ . Such reduction sometimes contains atomization steps - those hidden in the  $\varepsilon\epsilon\delta$ -reduction steps pertaining to the reduction. So the simulation in system  $\mathbf{F}$  by the Russell-Prawitz translation makes a controlled (not full) use of atomization depending on the source  $\mathbf{IPC}$  reduction step  $M \rightarrow N$ , while such a resource is not available in system  $\mathbf{F}_{\text{at}}$ , because in system  $\mathbf{F}_{\text{at}}$  we must stay fully atomized.



## Acknowledgements

The authors thank the referees for their comments, in particular, for an error pointed out in the first version of the proof of termination of atomization. Both authors were supported by Fundação para a Ciência e a Tecnologia [UIDB/00013/2020 and UIDP/00013/2020, UID/MAT/04561/2019, UID/CEC/00408/2019]. Both authors are grateful to Centro de Matemática, Aplicações Fundamentais e Investigação Operacional and the second author is also grateful to Large-Scale Informatics Systems Laboratory (Universidade de Lisboa).

## References

- [1] P. Aczel. The Russell-Prawitz modality. *Mathematical Structures in Computer Science*, 11(4):541–554, 2001.
- [2] E. S. Bainbridge, P. J. Freyd, A. Scedrov, and P. J. Scott. Functorial polymorphism. *Theor. Comput. Sci.*, 70(1):35–64, 1990.
- [3] J. Espírito Santo and G. Ferreira. A refined interpretation of intuitionistic logic by means of atomic polymorphism. *Studia Logica*, 2019. <https://doi.org/10.1007/s11225-019-09858-1>.
- [4] F. Ferreira. Comments on predicative logic. *Journal of Philosophical Logic*, 35:1–8, 2006.
- [5] F. Ferreira and G. Ferreira. Commuting conversions vs. the standard conversions of the “good” connectives. *Studia Logica*, 92:63–84, 2009.
- [6] G. Ferreira. Eta-conversions of **IPC** implemented in atomic **F**. *Logic Jnl IGPL*, 25(2):115–130, 2017.
- [7] J-Y. Girard, Y. Lafont, and P. Taylor. *Proofs and Types*. Cambridge University Press, 1989.
- [8] J. De Lataillade. Dinatural terms in system **F**. In *Proceedings of the 24th Annual IEEE Symposium on Logic in Computer Science, LICS 2009, 11-14 August 2009, Los Angeles, CA, USA*, pages 267–276. IEEE Computer Society, 2009.
- [9] P. Pistone, L. Tranchini, and M. Petrolo. The naturality of natural deduction (II). Some remarks on atomic polymorphism, 2019. arXiv:1908.11353.
- [10] D. Prawitz. *Natural Deduction. A Proof-Theoretical Study*. Almquist and Wiksell, Stockholm, 1965.
- [11] L. Tranchini, P. Pistone, and M. Petrolo. The naturality of natural deduction. *Studia Logica*, 107(1):195–231, 2019.
- [12] A. Troelstra and H. Schwichtenberg. *Basic Proof Theory*. Cambridge University Press, 1996.

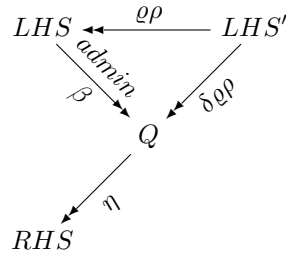
## A Some proofs

In this appendix we collect the proofs of Lemmas 4, 5 and 6.

**Lemma 4.** Let  $M \in \mathbf{F}_{\text{at}}$  and  $M' \in \mathbf{F}$  such that  $M' \rightarrow_{\varrho\rho}^* M$ .

$$\begin{aligned} LHS &= \underline{\text{case}}(M, x^A.\underline{\text{in}}_1(x, A, B), y^B.\underline{\text{in}}_2(y, A, B), A \vee B) \\ LHS' &= \underline{\text{CASE}}(M', x^A.\underline{\text{in}}_1(x, A, B), y^B.\underline{\text{in}}_2(y, A, B), A \vee B) \\ RHS &= M \end{aligned}$$

Then there is  $Q \in \mathbf{F}_{\text{at}}$  such that



*Proof.*  $LHS' \rightarrow_{\varrho\rho}^* LHS$  by  $M' \rightarrow_{\varrho\rho}^* M$  and Lemma 2.  $LHS$  is

$$\Lambda X.\underline{\text{case}}(M, x.(\Lambda Y \lambda z.z1x)X, y.(\Lambda Y \lambda z.z2y)X, ((A \supset X) \wedge (B \supset X)) \supset X)$$

From the proof of Lemma 6 in [3] we copy the following calculation, where we identify the term  $Q$ :

$$\begin{aligned} &LHS \\ \rightarrow_{\beta\vee}^2 &\Lambda X.\underline{\text{case}}(M, x.\lambda z.z1x, y.\lambda z.z2y, ((A \supset X) \wedge (B \supset X)) \supset X) \\ = &\Lambda X \lambda w.\underline{\text{case}}(M, x.(\lambda z.z1x)w, y.(\lambda z.z2y)w, X) \\ \rightarrow_{\beta\supset}^2 &\Lambda X \lambda w.\underline{\text{case}}(M, x.w1x, y.w2y, X) \\ = &\Lambda X \lambda w.MX \langle \lambda x.w1x, \lambda y.w2y \rangle =: Q \\ \rightarrow_{\eta\supset}^2 &\Lambda X \lambda w.MX \langle w1, w2 \rangle \\ \rightarrow_{\eta\wedge} &\Lambda X \lambda w.MXw \\ \rightarrow_{\eta\supset} &\Lambda X.MX \\ \rightarrow_{\eta\vee} &M \\ = &RHS \end{aligned}$$

We conclude as follows:

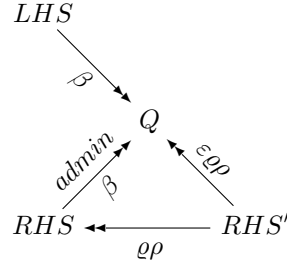
$$\begin{aligned} &LHS' \\ = &M'(A \vee B) \langle \lambda x^A \Lambda X \lambda w.w1x, \lambda y^B \Lambda X \lambda w.w2y \rangle \\ \rightarrow_{\varrho\rho}^* &M(A \vee B) \langle \lambda x^A \Lambda X \lambda w.w1x, \lambda y^B \Lambda X \lambda w.w2y \rangle \\ \rightarrow_{\delta} &\Lambda X.M(((A \supset X) \wedge (B \supset X)) \supset X) \langle \lambda x^A \lambda w.w1x, \lambda y^B \lambda w.w2y \rangle \\ \rightarrow_{\delta} &\Lambda X \lambda w.MX \langle \lambda x.w1x, \lambda y.w2y \rangle \\ = &Q \end{aligned}$$

□

**Lemma 5.** Let  $M, P_1, P_2, Q_1, Q_2 \in \mathbf{F}_{\text{at}}$  and  $M', P'_1, P'_2, Q'_1, Q'_2 \in \mathbf{F}$ . Let

$$\begin{aligned} LHS &= \underline{\text{case}}(\underline{\text{case}}(M, x_1^{A_1}.P_1, x_2^{A_2}.P_2, B_1 \vee B_2), y_1^{B_1}.Q_1, y_2^{B_2}.Q_2, C) \\ RHS &= \underline{\text{case}}(M, x_1.\underline{\text{case}}(P_1, y_1.Q_1, y_2.Q_2, C), x_2.\underline{\text{case}}(P_2, y_1.Q_1, y_2.Q_2, C), C) \\ RHS' &= \underline{\text{CASE}}(M', x_1.\underline{\text{CASE}}(P'_1, y_1.Q'_1, y_2.Q'_2, C), x_2.\underline{\text{CASE}}(P'_2, y_1.Q'_1, y_2.Q'_2, C), C) \end{aligned}$$

Suppose  $T' \rightarrow_{\varrho\rho}^* T$ , for  $T = M, P_1, P_2, Q_1, Q_2$ . Then, there is  $Q \in \mathbf{F}_{\text{at}}$  such that



*Proof.*  $RHS' \rightarrow_{\varrho\rho}^* RHS$  by the assumed reductions and Lemma 2. The remainder of the diagram is proved by induction on  $C$ .

Case  $C = Y$ .  $LHS$  is, by definition of case,

$$(\lambda X. \lambda w^{(B_1 \supset X) \wedge (B_2 \supset X)}. MX \langle \lambda x_1. P_1 X w, \lambda x_2. P_2 X w \rangle) Y \langle \lambda y_1. Q_1, \lambda y_2. Q_2 \rangle ,$$

which, after one  $\beta_{\vee}$ -reduction step, becomes

$$(\lambda w^{(B_1 \supset Y) \wedge (B_2 \supset Y)}. MY \langle \lambda x_1^{A_1}. P_1 Y w, \lambda x_2^{A_2}. P_2 Y w \rangle) \langle \lambda y_1^{B_1}. Q_1, \lambda y_2^{B_2}. Q_2 \rangle ,$$

because  $X \notin M, P_1, P_2, A_1, A_2, B_1, B_2$ . This term, in turn, yields, after one  $\beta_{\supset}$ -reduction step,

$$MY \langle \lambda x_1^{A_1}. P_1 Y \langle \lambda y_1. Q_1, \lambda y_2. Q_2 \rangle, \lambda x_2^{A_2}. P_2 Y \langle \lambda y_1^{B_1}. Q_1, \lambda y_2^{B_2}. Q_2 \rangle \rangle .$$

This is  $RHS$  by definition of case. This calculation comes from the proof of Lemma 11 in [3]. Now we add: put  $Q := RHS$ . The reduction  $RHS' \rightarrow_{\varepsilon\varrho\rho}^* Q$  holds due to  $RHS' \rightarrow_{\varrho\rho}^* RHS$ .

Case  $C = C_1 \supset C_2$ . By definition of case,  $LHS$  is  $\lambda z^{C_1}. LHS_0$ , where

$$LHS_0 = \underline{\text{case}}(\underline{\text{case}}(M, x_1.P_1, x_2.P_2, B_1 \vee B_2), y_1.Q_1 z, y_2.Q_2 z, C_2) .$$

On the other hand,  $RHS$  is, by definition of case,

$$\lambda z^{C_1}. \underline{\text{case}}(M, x_1.N_3, x_2.N_4, C_2) ,$$

with  $N_3 = (\underline{\text{case}}(P_1, y_1.Q_1, y_2.Q_2, C))z$ ,  $N_4 = (\underline{\text{case}}(P_2, y_1.Q_1, y_2.Q_2, C))z$ . As argued in the proof of Lemma 11 in [3],  $RHS$  does two administrative  $\beta_{\supset}$ -reduction steps (in the “wrong” direction), yielding  $\lambda z^{C_1}. RHS_0$ , where

$$RHS_0 = \underline{\text{case}}(M, x_1.N_1, x_2.N_2, C_2) ,$$

with  $N_1 = \underline{\text{case}}(P_1, y_1.Q_1z, y_2.Q_2z, C_2)$ ,  $N_2 = \underline{\text{case}}(P_2, y_1.Q_1z, y_2.Q_2z, C_2)$ .

Now  $RHS'$  is the term

$$M'(C_1 \supset C_2) \langle \lambda x_1. P'_1(C_1 \supset C_2) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle, \lambda x_2. P'_2(C_1 \supset C_2) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle \rangle$$

which, after one  $\varrho$ -reduction step, becomes

$$\lambda z^{C_1}. M' C_2 \langle \lambda x_1. (P'_1(C_1 \supset C_2) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle) z, \lambda x_2. (P'_2(C_1 \supset C_2) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle) z \rangle$$

After two  $\varepsilon$ -reduction steps one obtains

$$\lambda z^{C_1}. M' C_2 \langle \lambda x_1. P'_1 C_2 \langle \lambda y_1. Q'_1 z, \lambda y_2. Q'_2 z \rangle, \lambda x_2. P'_2 C_2 \langle \lambda y_1. Q'_1 z, \lambda y_2. Q'_2 z \rangle \rangle$$

The latter term is  $\lambda z^{C_1}. RHS'_0$ , where  $RHS'_0$  is

$$\underline{\text{CASE}}(M', x_1. \underline{\text{CASE}}(P'_1, y_1. Q'_1 z, y_2. Q'_2 z, C_2), x_2. \underline{\text{CASE}}(P'_2, y_1. Q'_1 z, y_2. Q'_2 z, C_2), C_2)$$

By IH, applied to the terms  $LHS_0$ ,  $RHS_0$  and  $RHS'_0$ , one obtains a term  $Q_0$  “in the middle” of three reduction sequences, as in the diagram above. The reduction relations involved are closed under the rule:  $T \rightarrow T' \Rightarrow \lambda z^{C_1}. T \rightarrow \lambda z^{C_1}. T'$ . So if we prefix the terms  $LHS_0$ ,  $RHS_0$ ,  $RHS'_0$  and  $Q_0$  with  $\lambda z^{C_1}$ , the same reductions hold. We take  $Q := \lambda z^{C_1}. Q_0$  and we are done.

Case  $C = C_1 \wedge C_2$ . By definition of  $\underline{\text{case}}$ ,  $LHS$  is  $\langle LHS_{0i} \rangle_{i=1,2}$ , where

$$LHS_{0i} = \underline{\text{case}}(\underline{\text{case}}(M, x_1. P_1, x_2. P_2, B_1 \vee B_2), y_1. Q_1 i, y_2. Q_2 i, C_i) .$$

On the other hand,  $RHS$  is, by definition of  $\underline{\text{case}}$ ,

$$\langle \underline{\text{case}}(M, x_1. N_3, x_2. N_4, C_i) \rangle_{i=1,2} ,$$

with  $N_3 = \underline{\text{case}}(P_1, y_1. Q_1, y_2. Q_2, C)i$  and  $N_4 = \underline{\text{case}}(P_2, y_1. Q_1, y_2. Q_2, C)i$ . As argued in the proof of Lemma 11 and in the comments on Theorem 1 in [3],  $RHS$  does four administrative  $\beta_\wedge$ -reduction steps (in the “wrong” direction), yielding the term  $\langle RHS_{0i} \rangle_{i=1,2}$ , where

$$RHS_{0i} = \underline{\text{case}}(M, x_1. N_1, x_2. N_2, C_i) ,$$

with  $N_1 = \underline{\text{case}}(P_1, y_1. Q_1 i, y_2. Q_2 i, C_i)$  and  $N_2 = \underline{\text{case}}(P_2, y_1. Q_1 i, y_2. Q_2 i, C_i)$ .

Now  $RHS'$  is the term

$$M'(C_1 \wedge C_2) \langle \lambda x_1. P'_1(C_1 \wedge C_2) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle, \lambda x_2. P'_2(C_1 \wedge C_2) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle \rangle$$

which, after one  $\varrho$ -reduction step, becomes

$$\langle M' C_i \langle \lambda x_1. (P'_1(C_1 \wedge C_2) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle) i, \lambda x_2. (P'_2(C_1 \wedge C_2) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle) i \rangle \rangle_{i=1,2}$$

After four  $\varepsilon$ -reduction steps, one obtains

$$\langle M' C_i \langle \lambda x_1. P'_1 C_i \langle \lambda y_1. Q'_1 i, \lambda y_2. Q'_2 i \rangle, \lambda x_2. P'_2 C_i \langle \lambda y_1. Q'_1 i, \lambda y_2. Q'_2 i \rangle \rangle \rangle_{i=1,2}$$

The latter term is  $\langle RHS'_{0i} \rangle_{i=1,2}$ , where  $RHS'_{0i}$  is

$$\underline{\text{CASE}}(M', x_1. \underline{\text{CASE}}(P'_1, y_1. Q'_1 i, y_2. Q'_2 i, C_i), x_2. \underline{\text{CASE}}(P'_2, y_1. Q'_1 i, y_2. Q'_2 i, C_i), C_i)$$

For each  $i = 1, 2$ , and by IH, applied to the terms  $LHS_{0i}$ ,  $RHS_{0i}$  and  $RHS'_{0i}$ , one obtains a term  $Q_{0i}$  “in the middle” of three reduction sequences, as in the diagram above. The reduction relations involved are closed under the rule:  $T_1 \rightarrow T'_1$  and  $T_2 \rightarrow T'_2 \Rightarrow \langle T_1, T_2 \rangle \rightarrow \langle T'_1, T'_2 \rangle$ . So if we form the pairs  $\langle LHS_{01}, LHS_{02} \rangle$ ,  $\langle RHS_{01}, RHS_{02} \rangle$ ,  $\langle RHS'_{01}, RHS'_{02} \rangle$  and  $\langle Q_{01}, Q_{02} \rangle$ , the same reductions hold. We take  $Q := \langle Q_{01}, Q_{02} \rangle$  and we are done.

Case  $C = \forall Y. D$ . By definition of case,  $LHS$  is  $\Lambda Y. LHS_0$ , where

$$LHS_0 = \underline{\text{case}}(\underline{\text{case}}(M, x_1. P_1, x_2. P_2, B_1 \vee B_2), y_1. Q_1 Y, y_2. Q_2 Y, D)$$

On the other hand,  $RHS$  is, by definition of case,

$$\Lambda Y. \underline{\text{case}}(M, x_1. N_3, x_2. N_4, D) ,$$

with  $N_3 = (\underline{\text{case}}(P_1, y_1. Q_1, y_2. Q_2, C))Y$ ,  $N_4 = (\underline{\text{case}}(P_2, y_1. Q_1, y_2. Q_2, C))Y$ . As argued in the proof of Lemma 11 in [3],  $RHS$  does two administrative  $\beta_{\forall}$ -reduction steps (in the “wrong” direction), yielding the term  $\Lambda Y. RHS_0$ , where

$$RHS_0 = \underline{\text{case}}(M, x_1. N_1, x_2. N_2, D) ,$$

with  $N_1 = \underline{\text{case}}(P_1, y_1. Q_1 Y, y_2. Q_2 Y, D)$ ,  $N_2 = \underline{\text{case}}(P_2, y_1. Q_1 Y, y_2. Q_2 Y, D)$ .

Now  $RHS'$  is

$$M'(\forall Y. D) \langle \lambda x_1. P'_1(\forall Y. D) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle, \lambda x_2. P'_2(\forall Y. D) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle \rangle$$

which, after a  $\varrho$ -reduction step, becomes

$$\Lambda Y. M' D \langle \lambda x_1. (P'_1(\forall Y. D) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle) Y, \lambda x_2. (P'_2(\forall Y. D) \langle \lambda y_1. Q'_1, \lambda y_2. Q'_2 \rangle) Y \rangle$$

After two  $\varepsilon$ -reduction steps, one obtains

$$\Lambda Y. M' D \langle \lambda x_1. P'_1 D \langle \lambda y_1. Q'_1 Y, \lambda y_2. Q'_2 Y \rangle, \lambda x_2. P'_2 D \langle \lambda y_1. Q'_1 Y, \lambda y_2. Q'_2 Y \rangle \rangle$$

The latter term is  $\Lambda Y. RHS'_0$ , where  $RHS'_0$  is

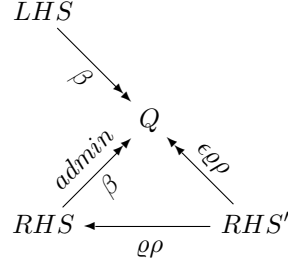
$$\underline{\text{CASE}}(M', x_1. \underline{\text{CASE}}(P'_1, y_1. Q'_1 Y, y_2. Q'_2 Y, D), x_2. \underline{\text{CASE}}(P'_2, y_1. Q'_1 Y, y_2. Q'_2 Y, D), D)$$

By IH, applied to the terms  $LHS_0$ ,  $RHS_0$  and  $RHS'_0$ , one obtains a term  $Q_0$  “in the middle” of three reduction sequences, as in the diagram above. The reduction relations involved are closed under the rule:  $T \rightarrow T' \Rightarrow \Lambda Y. T \rightarrow \Lambda Y. T'$ . So if we prefix the terms  $LHS_0$ ,  $RHS_0$ ,  $RHS'_0$  and  $Q_0$  with  $\Lambda Y$ , the same reductions hold. We take  $Q := \Lambda Y. Q_0$  and we are done.  $\square$

**Lemma 6.** Let  $M, P_1, P_2 \in \mathbf{F}_{\text{at}}$  and  $M', P'_1, P'_2 \in \mathbf{F}$ . Let

$$\begin{aligned} LHS &= \underline{\text{abort}}(\underline{\text{case}}(M, x_1^{A_1}. P_1, x_2^{A_2}. P_2, \perp), C) \\ RHS &= \underline{\text{case}}(M, x_1^{A_1}. \underline{\text{abort}}(P_1, C), x_2^{A_2}. \underline{\text{abort}}(P_2, C), C) \\ RHS' &= \underline{\text{CASE}}(M', x_1^{A_1}. \underline{\text{ABORT}}(P'_1, C), x_2^{A_2}. \underline{\text{ABORT}}(P'_2, C), C) \end{aligned}$$

Suppose  $T' \rightarrow_{\varrho\rho}^* T$ , for  $T = M, P_1, P_2$ . Then, there is  $Q \in \mathbf{F}_{\text{at}}$  such that



*Proof.*  $RHS' \rightarrow_{\varrho\rho}^* RHS$  by the assumed reductions and Lemmas 2 and 3. The remainder of the diagram is proved by induction on  $C$ .

Case  $C = Y$ .  $LHS$  is, by definition of abort and case,

$$(\Lambda X.MX \langle \lambda x_1^{A_1}.P_1X, \lambda x_2^{A_2}.P_2X \rangle)Y ,$$

which, after one  $\beta_Y$ -reduction step, becomes

$$MY \langle \lambda x_1^{A_1}.P_1Y, \lambda x_2^{A_2}.P_2Y \rangle ,$$

because  $X \notin M, P_1, P_2, A_1, A_2$ .

This is  $RHS$  by definition of abort and case. This calculation comes from the proof of Lemma 12 in [3]. Now we add: put  $Q := RHS$ . The reduction  $RHS' \rightarrow_{\epsilon\varrho\rho}^* Q$  holds due to  $RHS' \rightarrow_{\varrho\rho}^* RHS$ .

Case  $C = C_1 \supset C_2$ . By definition of abort,  $LHS$  is  $\lambda z^{C_1}.LHS_0$ , where

$$LHS_0 = \text{abort}(\text{case}(M, x_1.P_1, x_2.P_2, \perp), C_2) .$$

On the other hand,  $RHS$  is, by definition of case,

$$\lambda z^{C_1}.\text{case}(M, x_1.\text{abort}(P_1, C_1 \supset C_2)z, x_2.\text{abort}(P_2, C_1 \supset C_2)z, C_2) .$$

As argued in the proof of Lemma 12 and in the comments on Theorem 1 in [3],  $RHS$  does two administrative  $\beta_{\supset}$ -reduction steps (in the “wrong” direction), yielding  $\lambda z^{C_1}.RHS_0$ , where

$$RHS_0 = \text{case}(M, x_1.\text{abort}(P_1, C_2), x_2.\text{abort}(P_2, C_2), C_2) .$$

Now  $RHS'$  is the term

$$M'(C_1 \supset C_2) \langle \lambda x_1.P'_1(C_1 \supset C_2), \lambda x_2.P'_2(C_1 \supset C_2) \rangle$$

which, after one  $\varrho$ -reduction step, becomes

$$\lambda z^{C_1}.M'C_2 \langle \lambda x_1.P'_1(C_1 \supset C_2)z, \lambda x_2.P'_2(C_1 \supset C_2)z \rangle .$$

After two  $\epsilon$ -reduction steps one obtains

$$\lambda z^{C_1}.M'C_2 \langle \lambda x_1.P'_1C_2, \lambda x_2.P'_2C_2 \rangle .$$

The latter term is  $\lambda z^{C_1}.RHS'_0$ , where  $RHS'_0$  is

$$\text{CASE}(M', x_1.\text{ABORT}(P'_1, C_2), x_2.\text{ABORT}(P'_2, C_2), C_2).$$

By IH, applied to the terms  $LHS_0$ ,  $RHS_0$  and  $RHS'_0$ , one obtains a term  $Q_0$  “in the middle” of three reduction sequences, as in the diagram above. The reduction relations involved are closed under the rule:  $T \rightarrow T' \Rightarrow \lambda z^{C_1}.T \rightarrow \lambda z^{C_1}.T'$ . So if we prefix the terms  $LHS_0$ ,  $RHS_0$ ,  $RHS'_0$  and  $Q_0$  with  $\lambda z^{C_1}$ , the same reductions hold. We take  $Q := \lambda z^{C_1}.Q_0$  and we are done.

Case  $C = C_1 \wedge C_2$ . By definition of abort,  $LHS$  is  $\langle LHS_{0i} \rangle_{i=1,2}$ , where

$$LHS_{0i} = \text{abort}(\text{case}(M, x_1.P_1, x_2.P_2, \perp), C_i) .$$

On the other hand,  $RHS$  is, by definition of case,

$$\langle \text{case}(M, x_1.\text{abort}(P_1, C_1 \wedge C_2)i, x_2.\text{abort}(P_2, C_1 \wedge C_2)i, C_i) \rangle_{i=1,2} .$$

As argued in the proof of Lemma 12 and in the comments on Theorem 1 in [3],  $RHS$  does two administrative  $\beta_\wedge$ -reduction steps (in the “wrong” direction), yielding the term  $\langle RHS_{0i} \rangle_{i=1,2}$ , where

$$RHS_{0i} = \text{case}(M, x_1.\text{abort}(P_1, C_i), x_2.\text{abort}(P_2, C_i), C_i) .$$

Now  $RHS'$  is the term

$$M'(C_1 \wedge C_2) \langle \lambda x_1.P'_1(C_1 \wedge C_2), \lambda x_2.P'_2(C_1 \wedge C_2) \rangle$$

which, after one  $\varrho$ -reduction step, becomes

$$\langle M' C_i \langle \lambda x_1.P'_1(C_1 \wedge C_2)i, \lambda x_2.P'_2(C_1 \wedge C_2)i \rangle \rangle_{i=1,2}.$$

After two  $\epsilon$ -reduction steps one obtains

$$\langle M' C_i \langle \lambda x_1.P'_1 C_i, \lambda x_2.P'_2 C_i \rangle \rangle_{i=1,2}.$$

The latter term is  $\langle RHS'_{0i} \rangle_{i=1,2}$ , where  $RHS'_{0i}$  is

$$\text{CASE}(M', x_1.\text{ABORT}(P'_1, C_i), x_2.\text{ABORT}(P'_2, C_i), C_i).$$

For each  $i = 1, 2$ , and by IH, applied to the terms  $LHS_{0i}$ ,  $RHS_{0i}$  and  $RHS'_{0i}$ , one obtains a term  $Q_{0i}$  “in the middle” of three reduction sequences, as in the diagram above. The reduction relations involved are closed under the rule:  $T_1 \rightarrow T'_1$  and  $T_2 \rightarrow T'_2 \Rightarrow \langle T_1, T_2 \rangle \rightarrow \langle T'_1, T'_2 \rangle$ . So if we form the pairs  $\langle LHS_{01}, LHS_{02} \rangle$ ,  $\langle RHS_{01}, RHS_{02} \rangle$ ,  $\langle RHS'_{01}, RHS'_{02} \rangle$  and  $\langle Q_{01}, Q_{02} \rangle$ , the same reductions hold. We take  $Q := \langle Q_{01}, Q_{02} \rangle$  and we are done.

Case  $C = \forall Y.D$ . By definition of abort,  $LHS$  is  $\Lambda Y.LHS_0$ , where

$$LHS_0 = \text{abort}(\text{case}(M, x_1.P_1, x_2.P_2, \perp), D).$$

On the other hand,  $RHS$  is, by definition of case,

$$\Lambda Y. \text{case}(M, x_1. \text{abort}(P_1, \forall Y. D)Y, x_2. \text{abort}(P_2, \forall Y. D)Y, D) \ .$$

As argued in the proof of Lemma 12 in [3],  $RHS$  does two administrative  $\beta_{\forall}$ -reduction steps (in the “wrong” direction), yielding the term  $\Lambda Y. RHS_0$ , where

$$RHS_0 = \text{case}(M, x_1. \text{abort}(P_1, D), x_2. \text{abort}(P_2, D), D) \ .$$

Now  $RHS'$  is

$$M'(\forall Y. D) \langle \lambda x_1. P'_1(\forall Y. D), \lambda x_2. P'_2(\forall Y. D) \rangle$$

which, after a  $\varrho$ -reduction step, becomes

$$\Lambda Y. M' D \langle \lambda x_1. (P'_1(\forall Y. D))Y, \lambda x_2. (P'_2(\forall Y. D))Y \rangle.$$

After two  $\epsilon$ -reduction steps, one obtains

$$\Lambda Y. M' D \langle \lambda x_1. P'_1 D, \lambda x_2. P'_2 D \rangle.$$

The latter term is  $\Lambda Y. RHS'_0$ , where  $RHS'_0$  is

$$\text{CASE}(M', x_1. \text{ABORT}(P'_1, D), x_2. \text{ABORT}(P'_2, D), D).$$

By IH, applied to the terms  $LHS_0$ ,  $RHS_0$  and  $RHS'_0$ , one obtains a term  $Q_0$  “in the middle” of three reduction sequences, as in the diagram above. The reduction relations involved are closed under the rule:  $T \rightarrow T' \Rightarrow \Lambda Y. T \rightarrow \Lambda Y. T'$ . So if we prefix the terms  $LHS_0$ ,  $RHS_0$ ,  $RHS'_0$  and  $Q_0$  with  $\Lambda Y$ , the same reductions hold. We take  $Q := \Lambda Y. Q_0$  and we are done. □