Natural Deduction in Classical First-Order Logic: Exceptions, Strong Normalization and Herbrand's Theorem

Federico Aschieri, Margherita Zorzi

Natural Deduction in Classical First-Order Logic: Exceptions, Strong Normalization and Herbrand's Theorem

Federico Aschieri[*1] **and Margherita Zorzi**[†2]

1 **Laboratoire de l'Informatique du Parallélisme (UMR 5668, CNRS, UCBL) École Normale Supérieure de Lyon – Université de Lyon, France**
2 **Dipartimento di Informatica, Università di Verona, Italy**

Abstract

We present a new Curry-Howard correspondence for classical first-order natural deduction. We add to the lambda calculus an operator which represents, from the viewpoint of programming, a mechanism for raising and catching multiple exceptions, and from the viewpoint of logic, the excluded middle over arbitrary prenex formulas. The machinery will allow to extend the idea of learning – originally developed in Arithmetic – to pure logic. We prove that our typed calculus is strongly normalizing and show that proof terms for simply existential statements reduce to a list of individual terms forming a Herbrand disjunction. A by-product of our approach is a natural-deduction proof and a computational interpretation of Herbrand's Theorem.

1998 ACM Subject Classification F.4.1

Keywords and phrases classical first-order logic, natural deduction, Herbrand theorem, delimited exceptions, Curry-Howard correspondence

1 Introduction

In the midst of an age of baffling paradoxes and contradictions, during the heat of a harsh controversy between opposed approaches to foundations of mathematics – infinitism vs. constructivism – it must have been required a new and really penetrating insight to see a way out. Hilbert's proposed solution, at the beginning of twentieth century, was certainly deep and brilliant. According to him, there was no contradiction between classical and intuitionistic mathematics, because the ideal objects and principles that appear in classical reasoning can always be eliminated after having proved some concrete, incontestably meaningful statement. Hilbert's idea was made precise in its *epsilon substitution method* (see[22]), a systematic procedure to eliminate ideal objects from classical proofs and reduce every logical step to a concrete calculation. Hilbert's program was to show the termination of his method, or variants thereof, initially for first-order classical logic, then Peano Arithmetic and finally Analysis. As it turned out, Hilbert was right, and some termination proofs have been provided for example by Ackermann (for a modern proof see [22]) and Mints [23].

* This work was supported by the LABEX MILYON (ANR-10-LABX-0070) of Université de Lyon, within the program "Investissements d'Avenir" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR)
† Partially supported by LINTEL (Linear Techniques For The Analysis of Languages), https://sites.google.com/site/tolintel/

1.1 Herbrand's and Kreisel's Theorems

After Hilbert, two other seminal results had been obtained stating that it is always possible to eliminate non-constructive reasoning in two important logical systems.

- The first one is *Herbrand's Theorem* [11], which says that if a simply existential statement $\exists\alpha\,\mathsf{P}$ is derivable in classical first-order logic from a set of purely universal premises, then there is sequence of terms $m_1, m_2, \ldots, m_k$ such that the *Herbrand disjunction* $\mathsf{P}[m_1/\alpha] \vee \mathsf{P}[m_2/\alpha] \vee \ldots \vee \mathsf{P}[m_k/\alpha]$ is provable in classical propositional logic from a set of instances of the premises.
- The second one is *Kreisel's Theorem* [20], which says that if a simply existential formula $\exists\alpha\,\mathsf{P}$ is derivable in classical first-order Arithmetic, then it is derivable already in intuitionistic first-order Arithmetic. Using Kreisel's modified realizability [21] (or many other techniques), one can compute out of the intuitionistic proof a number n – a witness – such that $\mathsf{P}[n/\alpha]$ is true, whenever $\mathsf{P}[n/\alpha]$ it is closed.

Both Herbrand's and Kreisel's proof techniques are now obsolete, but the meaning of their results is as valid as ever, because it provides a theoretical justification for an important quest: the search for the constructive content of classical proofs. Herbrand's Theorem tells us what is the immediate computational content of classical first-order logic: the list of witnesses contained in any Herbrand disjunction. Kreisel's Theorem tells us what is the immediate computational content of first-order Arithmetic: the numeric witness for any provable existential statement. What is of great interest, in the light of those results, is to automatically transform proofs into programs in order to compute from any proof of any existential statement a suitable list of witnesses, in first-order logic, a single witness, in Arithmetic. In this paper, we shall address the first-order version of the problem – and propose a new solution.

1.2 Natural Deduction and Sequent Calculus

The two most successful and most studied deductive systems for first-order logic are Gentzen's natural deduction [24] and Gentzen's sequent calculus [16, 15]. The first elegant constructive proof of Herbrand's Theorem was indeed obtained as a corollary of Gentzen's Cut elimination Theorem. Today, that proof is still the most cited and the most used. On the contrary, we even failed to find in the literature a complete proof of Herbrand's Theorem using classical natural deduction. This is no coincidence, but yet another instance of the legendary duality between the two formalisms: as a matter of fact, some results are much more easily discovered and proved in the sequent calculus, while other are far more easily obtained in natural deduction. Since the time of Gentzen, natural deduction worked seamlessly for intuitionistic logic, and led to the discovery of the Curry-Howard correspondence [25], while sequent calculus was much more technically convenient in classical logic (Gentzen was not able to prove a meaningful normalization theorem for classical natural deduction, whilst he *was* for the intuitionistic case [26]). It indeed took a surprisingly long time to discover suitable reduction rules for classical natural deduction systems with all connectives [18] (see also [7, 25] for a more detailed history).

The great advantage of using natural deduction instead of sequent calculus is no mystery: it is *natural*! When logically solving non-trivial problems, humans adopt forward reasoning, which is more adapted to *proof-construction*: one starts from some observations, draws some consequences and gradually combine them so to reach the goal. On the other hand, sequent calculus is more suitable for machine-like *proof-search*: one start from the final goal and applies mechanically logical rules to reach axioms. As a consequence, when analyzing real

mathematical proofs so to investigate their constructive content, one likes it better to use natural deduction. Moreover, the reduction of a proof into normal form is nothing but the evaluation of a functional program, and so very easy to understand. The cut-elimination process, instead, is far more involved and difficult to follow. For example, the proof of Herbrand's Theorem by cut-elimination is deceptively simple: while it is rather obvious that the final cut-free proof contains an Herbrand disjunction, it is very painful to gain a step-by-step and clear understanding of how the corresponding list of witnesses has been produced.

1.3 Classical Natural Deduction: an Exception-Based Curry-Howard Correspondence

We would like to endow classical first-order natural deduction with a *natural* set of reduction rules that also allows a *natural, seamless* proof of Herbrand's Theorem. As a corollary, this system would also have a simple and meaningful computational interpretation. Indeed, we believe that one can say to really understand a theorem when one is able to construct a proof of it that, a posteriori, appears completely natural, almost obvious. Usually, that happens when one has created a framework of concepts and methods that *explain* the theorem.

1.3.1 EM_1 and Exceptions in Arithmetic

If one wants to understand how is it possible that a classical proof has any computational content in the first place, the concept of *learning* is essential. It was a Hilbert discovery that from classical proofs one can extract approximation processes, that learn how to constructs non-effective objects by an intelligent process of trial and error. More recently, Interactive realizability [2, 9, 3, 4, 5] has been developed, which is a framework that finally combines the learning idea with the formulae-as-types tradition. In [7] a Curry-Howard correspondence for a classical system of Arithmetic is introduced: namely, Heyting Arithmetic HA with the excluded middle schema EM_1, $\forall\alpha\mathsf{P} \vee \exists\alpha\neg\mathsf{P}$, where P is any atomic, and *hence decidable*, predicate. Classical programs are described as programs that *make hypotheses*, *test them* and *correct them* when they are *learned* to be wrong. In particular, EM_1 is treated as an elimination rule:

$$\frac{\Gamma, a : \forall\alpha\,\mathsf{P} \vdash u : C \qquad \Gamma, a : \exists\alpha\,\neg\mathsf{P} \vdash v : C}{\Gamma \vdash u \parallel_a v : C}$$

This inference is nothing but a familiar disjunction elimination rule, where the main premise EM_1 has been cut, since, being a classical axiom, it has no computational content in itself. The proof terms u, v are both kept as possible alternatives, since one is not able to decide which branch is going to be executed at the end.

The informal idea expressed by the associated reductions is to assume $\forall\alpha\,\mathsf{P}$ and try to produce some *complete* proof of C out of u by reducing inside u. Whenever u needs the truth of an instance $\mathsf{P}[n/\alpha]$ of the assumption $\forall\alpha\,\mathsf{P}$, it checks it, and if it is true, it replaces it by its canonical proof which is just a computation. If all instances $\mathsf{P}[n/\alpha]$ of $\forall\alpha\,\mathsf{P}$ being checked are true, *and no assumption* $\forall\alpha\mathsf{P}$ *is left* (this is the non-trivial part), then the normal form u' of u is *independent* from $\forall\alpha\,\mathsf{P}$ and we found some $u' : C$. If instead some assumption of $\forall\alpha\mathsf{P}$ is left in u, one may encounter some instance $\mathsf{P}[n/\alpha]$ which is false, and thus refute the assumption $\forall\alpha\,\mathsf{P}$. In this case the attempt of proving C from $\forall\alpha\mathsf{P}$ fails, one obtains $\neg\mathsf{P}[n/\alpha]$ and u *raises the exception* n; from the knowledge that $\neg\mathsf{P}[n/\alpha]$ holds, a canonical proof term

$\exists\alpha\,\neg\mathsf{P}$ is formed and passed to v: a proof term for C has now been obtained and it can be executed.

1.3.2 EM_n and Exceptions in Classical Logic

Our goal is to extend the learning methods developed for $\mathsf{HA}+\mathsf{EM}_1$ to classical first-order logic. There is a catch: the reductions we have just described do no longer work! The obvious obstacle is that it is not possible to check the truth of formulas, even of atomic ones: there is no such a thing as a standard model for classical first-order logic, let alone an absolute notion of truth. Is the whole idea of learning bound to fail and be abandoned or it can be rescued in some way? The problem is that, even though classical first-order logic is proof-theoretically much weaker than first-order Arithmetic, in a sense, it is harder to interpret and gives rise to different issues. The programs extracted from proofs in $\mathsf{HA}+\mathsf{EM}_1$ explore many possible computational paths, due to the bifurcations produced by EM_1. When the proven formula is a simply existential statement, either a path will succeed in finding a correct witness or will fail and throw some information which will activate another path. At the very end, a single computational path will find a witness. Herbrand's Theorem for classical first-order logic, instead, asserts only the existence of a *list of possible witnesses* for the proven existential formula. This must be due to the fact that it is often impossible to solve the dilemmas that are posed by the use of the exclude middle, and several alternatives computational paths are to be kept forever in parallel.

Let us consider again the rule for EM_1, but now in pure first-order logic:

$$\frac{\Gamma, a:\forall\alpha\,\mathsf{P}\vdash u:C \qquad \Gamma, a:\exists\alpha\,\neg\mathsf{P}\vdash v:C}{\Gamma\vdash u\parallel_a v:C}\,\mathsf{EM}_1$$

The idea is still to start reducing inside u in order to produce a proof of C. But the first time one needs an instance $\mathsf{P}[m/\alpha]$ of the hypothesis $\forall\alpha\,\mathsf{P}$ to hold, where m is now a first-order term, an exception is automatically thrown. Since one is not able to decide whether $\mathsf{P}[m/\alpha]$ holds, the current universe *doubles* and a new pair of parallel, mutually exclusive universes is generated. In the first one, $\mathsf{P}[m/\alpha]$ is supposed to hold, in the second one, $\neg\mathsf{P}[m/\alpha]$ is supposed to. What is the correct universe? One shall never know, and parallel reductions must continue to be made in these two universes. In the first one, *inside* u, a small progress has been made, because a use of the universal hypothesis $\forall\alpha\,\mathsf{P}$ can be eliminated: $\mathsf{P}[m/\alpha]$ holds by the very hypothesis that generated the universe, and it is no longer necessary to justify it as a consequence of $\forall\alpha\,\mathsf{P}$. Hence u can reduce to the term u^- obtained by erasing the premise $\forall\alpha\,\mathsf{P}$ of all eliminations of $\forall\alpha\,\mathsf{P}$ having as conclusion $\mathsf{P}[m/\alpha]$. In the second one, *inside* v, a considerable progress has been made, since a witness m for $\exists\alpha\,\neg\mathsf{P}$ has been *learned*, again by the very hypothesis that generated the universe. Hence v can reduce to the term v^+ obtained by replacing all occurrences of the hypothesis $\exists\alpha\,\neg\mathsf{P}$ with a proof of it by an introduction rule with premise $\neg\mathsf{P}[m/\alpha]$. The generation of the two universes is logically supported by the use of the excluded middle EM_0 over propositional formulas, which has the general form:

$$\frac{\Gamma, b:\neg\mathsf{Q}\vdash w_1:D \qquad \Gamma, b:\mathsf{Q}\vdash w_2:D}{\Gamma\vdash w_1\mid w_2:D}\,\mathsf{EM}_0$$

The resulting conversion for the conclusion $u\parallel_a v$ of EM_1 is the following:

$$\dfrac{\Gamma, b:\neg\mathsf{P}[m/\alpha]\vdash v^+:C \qquad \dfrac{\Gamma, a:\forall\alpha\,\mathsf{P}, b:\mathsf{P}[m/\alpha]\vdash u^-:C \qquad \Gamma, a:\exists\alpha\,\neg\mathsf{P}\vdash v:C}{\Gamma, b:\mathsf{P}[m/\alpha]\vdash u^-\parallel_a v:C}\,\mathsf{EM}_1}{\Gamma\vdash v^+\mid(u^-\parallel_a v):C}\,\mathsf{EM}_0$$

We see that in the term $v^+ \mid (u^- \parallel_a v)$, there is a single bar $\mid$ separating forever v^+ and $(u^- \parallel_a v)$: the two terms will give rise to two different and independent computations. In the first, a universal hypothesis has been *confirmed*, in the second, the same universal hypothesis has been *refuted* and a counterexample *learned*: the idea of learning has been saved!

The term $u \,|||_a\, v$ decorating the conclusion of excluded middle EM_2

$$\frac{\Gamma, a : \forall\alpha\,\exists\beta\,\mathsf{P} \vdash u : C \qquad \Gamma, a : \exists\alpha\,\forall\beta\,\neg\mathsf{P} \vdash v : C}{\Gamma \vdash u \,|||_a\, v : C}\ \mathsf{EM}_2$$

will reduce, in a completely equivalent fashion, to

$$\dfrac{\Gamma, b : \forall\beta\neg\mathsf{P}[m/\alpha] \vdash v^+ : C \qquad \dfrac{\Gamma, a : \forall\alpha\,\exists\beta\,\mathsf{P}, b : \exists\beta\,\mathsf{P}[m/\alpha] \vdash u^- : C \qquad \Gamma, a : \exists\alpha\,\forall\beta\,\neg\mathsf{P} \vdash v : C}{\Gamma, b : \exists\beta\,\mathsf{P}[m/\alpha] \vdash u^- \,|||_a\, v : C}\ \mathsf{EM}_2}{\Gamma \vdash v^+ \parallel_b (u^- \,|||_a\, v) : C}\ \mathsf{EM}_1$$

u^- is now obtained from u by erasing the premise $\forall\alpha\,\exists\beta\,\mathsf{P}$ of all eliminations of $\forall\alpha\,\exists\beta\,\mathsf{P}$ having as conclusion $\exists\beta\,\mathsf{P}[m/\alpha]$; v^+ is obtained by replacing all occurrences of the hypothesis $\exists\alpha\,\forall\beta\,\neg\mathsf{P}$ with a proof of it by an introduction rule with premise $\forall\beta\,\neg\mathsf{P}[m/\alpha]$. This time the generation of the new pair of universes in the term $v^+ \parallel_b (u^- \,|||_a\, v)$ is logically supported by EM_1, so the number of bars in the last application of EM is two, decreasing by one. Therefore, the two universes are parallel, but can still communicate with each other: an exception may at any moment by raised by v^+ and a term be passed in particular to u^-. This will be very useful, since the hypothesis $b : \exists\beta\,\mathsf{P}[m/\alpha]$ may block the computation inside u^-.

The reduction rules for the excluded middle on prenex formulas with n alternating quantifiers – EM_n – are the obvious generalization of what we have just explained: for full details see Section §2. The general idea is that the right $\exists$-branch of the excluded middle always waits for a witness coming from the left $\forall$-branch. These two universes are completely separated, but inhabitants of the second can receive "divine gifts" from the first, under the form of possible witnesses. The inhabitants of the second universe cannot see how these godsends are produced, and may accept them as manifestation of divine providence. This should remind the reader the copycat strategy for EM_n in Coquand's game semantics [12].

In order to implement our reductions we shall use constant terms of the form $\mathtt{H}_a^{\forall\alpha A}$, whose task is to automatically raise an exception: the notation $\mathsf{raise}_a^{\forall\alpha A}$ would also have been just fine. We shall also use a constant $\mathtt{W}_a^{\exists\alpha A^\perp}$ denoting some unknown proof term for $\exists\alpha A^\perp$ ($A^\perp$ is the usual involutive negation), whose task is to *catch* the exception raised by $\mathtt{H}_a^{\forall\alpha P}$. Actually, these terms will occur only through typing rules of the form

$$\Gamma, a : \forall\alpha A \vdash \mathtt{H}_a^{\forall\alpha A} : \forall\alpha A \qquad \Gamma, a : \exists\alpha A^\perp \vdash \mathtt{W}_a^{\exists\alpha A^\perp} : \exists\alpha A^\perp$$

where a is used just as a name of a communication channel for exceptions: if in u occurs a subterm of the form $\mathtt{H}_a^{\forall\alpha A} m$, then in an exception is raised in $u \,\|_a\, v$ and passed to v ($\|$ stands for a sequence of $n+1$ bars in the case of EM_n). From the viewpoint of programming, that is a *delimited exception* mechanism (see de Groote [17] and Herbelin [19] for a comparison). The scope of an exception has the form $u \parallel_a v : C$, with u the "ordinary" part of the computation and v the "exceptional" part. Similar mechanism are expressed by the constructs raise and $\mathsf{try} \ldots \mathsf{with} \ldots$ in the CAML programming language. There is a substantial difference, however, with the exception handling mechanism used in [7]. Here, the ordinary part of the computation goes on after the first exception, and in fact can raise *multiple* exceptions, one after another, which are all passed to the exception handler; in [7], instead, the ordinary part of the computation is aborted *as soon as* the first exception is raised.

1.3.3 Permutation Rules

A problem arises when the conclusion C of the excluded middle is employed as the main premise of an elimination rule to obtain some new conclusion. For example, already with EM_0, when $C = A \to B$, and $\Gamma \vdash w : A$, one may form the proof term $(w_1 \mid w_2)w$ of type B. In this case, one may not be able to solve the dilemma of choosing between w_1 and w_2, and the computation may not evolve further: one is stuck.

As in [7], the problem is solved by adding Prawitz's permutation rules [24], as usual with disjunction. For example, $(u \mid v)w$ reduces to $uw \mid vw$. In this way, one obtains two important results: first, one may explore *both* the possibilities, $\forall\alpha\mathsf{P}$ holds or $\exists\alpha\neg\mathsf{P}$ holds, and evaluate uw and vw; second, one duplicates the applicative context $[\,]w$. If $C = A \wedge B$, one may form the proof term $\pi_0(u \mid v)$, which reduces to $\pi_0 u \mid \pi_0 v$, and has the effect of duplicating the context $\pi_0[\,]$. Similar standard considerations hold for the other connectives. Thus permutation rules act similarly to the rules for μ in the $\lambda\mu$-calculus, but are only used to *duplicate* step-by-step the context and produce implicitly the continuation. Anyway, $\mid$ behaves like a control-like operator.

1.3.4 Herbrand's Disjunction Extraction and Strong Normalization

The computational content of a classical first-order proof of a simply existential statement is the list of witnesses appearing in a Herbrand disjunction. Why in intuitionistic logic the result of the normalization process is a *single* witness, while in classical logic it is just a *list of possibilities*? The reduction rules for EM provide an intuitive explanation of *why* this list is produced and highlight each of the moments *when* a piece of it is built. During the normalization of a proof term, the computation is first purely intuitionistic and heading towards a single witness. In other terms, only redexes of the standard lambda calculus are at first contracted. However, the computation may be blocked by an instance of a universal hypothesis $\mathtt{H}_a^{\forall\alpha A} m$ which the program cannot decide. At that time, the universe doubles, but in each of new pair of universes, the computation goes on and stays intuitionistic. In each of the two universes, new universe duplications can occur and so on .... At the very end, there will be several different intuitionistic computations: each of them will produce, as expected, a witness, and the collection of all of them will form the Herbrand disjunction. This intuitive description will be formalized in a *normal form property* that we shall prove.

We shall also prove a *strong normalization* result stating that every reduction path generated by any proof term will terminate in a normal form. We shall employ a non-deterministic technique introduced in [6], in turn inspired by [8]. While the strong normalization result in [7] was obtained by means of a special notion of realizability, we had considerable troubles generalizing that technique. At the end, the non-deterministic approach revealed much more simple to generalize. We thus leave open the interesting problem of defining a realizability or a proof-theoretic semantics for our natural deduction system.

1.4 Plan of the Paper

This is the plan of the paper. In Section §2 we introduce a type-theoretical version of intuitionistic first-order logic IL extended with $\mathsf{EM} := \bigcup_n \mathsf{EM}_n$. In Section §3 we prove the strong normalization of a non-deterministic variant $\mathsf{IL} + \mathsf{EM}^\star$ of $\mathsf{IL} + \mathsf{EM}$, which immediately implies the strong normalization of the latter. In Section §4, we prove that from any quasi-closed term having as type a simply existential formula, one can extract a correspondent Herbrand disjunction.

2 The System IL + EM

In this section we describe a standard natural deduction system for intuitionistic first-order logic IL, with a term assignment based on Curry-Howard correspondence (see [25] e.g.). We extend the system with an operator which formalizes the excluded middle principle EM_n.

We start with the standard first-order language of formulas.

■ **Definition 1** (Language of IL + EM)**.** The language $\mathcal{L}$ of IL + EM is defined as follows.

1. The terms of $\mathcal{L}$ are inductively defined as either variables $\alpha, \beta, \ldots$ or constants c or expressions of the form $\mathsf{f}(t_1, \ldots, t_n)$, with f function constant of arity n and $t_1, \ldots, t_n \in \mathcal{L}$.
2. There is a countable set of *predicate symbols*. The *atomic formulas* of $\mathcal{L}$ are all the expressions of the form $\mathcal{P}(t_1, \ldots, t_n)$ such that $\mathcal{P}$ is a predicate symbol of arity n and $t_1, \ldots, t_n$ are terms of $\mathcal{L}$. We assume to have a 0-ary predicate symbol $\bot$ which represents falsity.
3. The formulas of $\mathcal{L}$ are built from atomic formulas of $\mathcal{L}$ by the logical constants $\vee, \wedge, \to, \forall, \exists$, with quantifiers ranging over variables $\alpha, \beta, \ldots$: if A, B are formulas, then $A \wedge B$, $A \vee B$, $A \to B$, $\forall\alpha\, A$, $\exists\alpha\, B$ are formulas. The logical negation $\neg A$ can be introduced, as usual, as an abbreviation of the formula $A \to \bot$
4. *Propositional formulas* are the formulas whose only logical constants are $\wedge, \vee, \to$; we say that a propositional formula is *negative* whenever $\vee$ does not occur in it. Propositional formulas will be denoted as $\mathsf{P}, \mathsf{Q} \ldots$ (possibly indexed). Formulas of the form $\forall\alpha_1 \ldots \forall\alpha_n\, \mathsf{P}$, with $n \geq 0$ and P propositional, will be denoted as $\forall\vec{\alpha}\, \mathsf{P}$ and will be called *purely universal*; if P is also negative, the formula will be called *simply universal*.

For deducing the axiom $\bot \to A$ (ex falso sequitur quodlibet), it is enough to have $\bot \to \mathsf{P}$, where P is atomic, and the axioms of equality as well can be formulated as simply universal. They will not appear explicitly in the logical rules, since at any rate we shall have to treat a more general case: the computational interpretation of proofs having as assumptions an arbitrary set of simply universal statements, as usual in Herbrand's Theorem.

We now define in Figure 1 a set of untyped proof terms, then a type assignment for them.

We assume that in the proof terms three distinct classes of variables appear: one is made by the variables for the terms themselves, denoted usually as $x, y, \ldots$; one is made by the quantified variables of the formula language $\mathcal{L}$ of IL + EM, denoted usually as $\alpha, \beta, \ldots$; one is made by the hypothesis variables, for the pair of hypotheses bound by EM_n, denoted usually as $a, b, \ldots$.

We formalize each instance of the Excluded Middle principle on prenex formulas EM_n with n alternating quantifiers by terms of the form $u \underbrace{|\,|\,\ldots|_a}_{n+1} v$, where a is a hypothesis variable which explicitly appears in the premisses bounded by the EM_n rule. We will call a *bar* any symbol of the shape $|$. In the following, we exploit the compact notation $\mathbf{|}$ in order to denote an arbitrary sequence of n bars $|$. The symbol $\mathbf{\|}$ stands for $n+1$ bars whenever $\mathbf{|}$ represents a sequence of n bars.

In the term $u \mathbf{|}_a v$, any free occurrence of a in u occurs in an expression $\mathtt{H}_a^{\forall\alpha A}$, and denotes an hypothesis $\forall\alpha A$. Any free occurrence of a in v occurs in an expression $\mathtt{W}_a^{\exists\alpha A}$, and denotes an hypothesis $\exists\alpha A$. All the free occurrences of a in u and v are bound in $u \mathbf{|}_a v$. $\mathtt{H}_a^{\forall\alpha A}$ is the *thrower* of an exception n (related to the hypothesis variable a, see Definition 2) and $\mathtt{W}_a^{\exists\alpha A}$ is the *catcher* of the same exception n. In the terms $\mathtt{H}_a^{\forall\alpha A}$ and $\mathtt{W}_a^{\exists\alpha A}$

Grammar of Untyped Proof Terms

$$t, u, v ::= x \mid tu \mid tm \mid \lambda x\, u \mid \lambda \alpha\, u \mid \langle t, u\rangle \mid u\,\pi_0 \mid u\,\pi_1 \mid \iota_0(u) \mid \iota_1(u) \mid t[x.u, y.v] \mid (m, t) \mid t[(\alpha, x).u]$$
$$\mid (u \mid v) \mid u \underbrace{\mid\mid \ldots \mid_a}_{n+1 bars} v \mid \mathtt{H}_a^{\forall\alpha A} \mid \mathtt{W}_a^{\exists\alpha A} \mid \mathtt{H}^{\mathsf{P}}$$

where m ranges over terms of $\mathcal{L}$, x over proof-term variables, a over hypothesis variables and A is a prenex formula with negative propositional matrix or is a simply universal formula. We assume that in the term $u \underbrace{\mid\mid \ldots \mid_a}_{n+1} v$, there is some formula A, such that a occurs free in u only in subterms of the form $\mathtt{H}_a^{\forall\alpha A}$ and a occurs free in v only in subterms of the form $\mathtt{W}_a^{\exists\alpha A}$, and the occurrences of the variables in A different from α are free in both u and v.

Contexts With Γ we denote contexts of the form $e_1 : A_1, \ldots, e_n : A_n$, where each e_i is either a proof-term variable $x, y, z \ldots$ or a EM hypothesis variable $a, b, \ldots$, and $e_i \neq e_j$ for $i \neq j$.

Axioms $\Gamma, x : A \vdash x : A$ $\quad \Gamma, a : \forall\alpha\, A \vdash \mathtt{H}_a^{\forall\alpha A} : \forall\alpha\, A$ $\quad \Gamma, a : \exists\alpha\, A \vdash \mathtt{W}_a^{\exists\alpha A} : \exists\alpha\, A$
$\Gamma, a : \mathsf{P} \vdash \mathtt{H}^{\mathsf{P}} : \mathsf{P}$

Conjunction $\dfrac{\Gamma \vdash u : A \quad \Gamma \vdash t : B}{\Gamma \vdash \langle u, t\rangle : A \wedge B}$ $\quad \dfrac{\Gamma \vdash u : A \wedge B}{\Gamma \vdash u\,\pi_0 : A}$ $\quad \dfrac{\Gamma \vdash u : A \wedge B}{\Gamma \vdash u\,\pi_1 : B}$

Implication $\dfrac{\Gamma \vdash t : A \to B \quad \Gamma \vdash u : A}{\Gamma \vdash tu : B}$ $\quad \dfrac{\Gamma, x : A \vdash u : B}{\Gamma \vdash \lambda x\, u : A \to B}$

Disjunction Introduction $\dfrac{\Gamma \vdash u : A}{\Gamma \vdash \iota_0(u) : A \vee B}$ $\quad \dfrac{\Gamma \vdash u : B}{\Gamma \vdash \iota_1(u) : A \vee B}$

Disjunction Elimination $\dfrac{\Gamma \vdash u : A \vee B \quad \Gamma, x : A \vdash w_1 : C \quad \Gamma, x : B \vdash w_2 : C}{\Gamma \vdash u\,[x.w_1, x.w_2] : C}$

Universal Quantification $\dfrac{\Gamma \vdash u : \forall\alpha A}{\Gamma \vdash um : A[m/\alpha]}$ $\quad \dfrac{\Gamma \vdash u : A}{\Gamma \vdash \lambda\alpha\, u : \forall\alpha A}$

where m is any term of the language $\mathcal{L}$ and α does not occur free in any formula B occurring in Γ.

Existential Quantification $\dfrac{\Gamma \vdash u : A[m/\alpha]}{\Gamma \vdash (m, u) : \exists\alpha A}$ $\quad \dfrac{\Gamma \vdash u : \exists\alpha A \quad \Gamma, x : A \vdash t : C}{\Gamma \vdash u\,[(\alpha, x).t] : C}$

where α is not free in C nor in any formula B occurring in Γ.

EM_0 $\dfrac{\Gamma, a : \neg\mathsf{P} \vdash u : C \quad \Gamma, a : \mathsf{P} \vdash v : C}{\Gamma \vdash u \mid v : C}$ (P negative)

$\mathsf{EM}n$ $\dfrac{\Gamma, a : \forall\alpha\, A \vdash u : C \quad \Gamma, a : \exists\alpha\, A^{\perp} \vdash v : C}{\Gamma \vdash u \underbrace{\mid\mid \ldots \mid_a}_{n+1} v : C}$

where $A = \exists\alpha_0\, \forall\alpha_1 \exists\alpha_2 \ldots \forall\alpha_{n-2} \exists\alpha_{n-1}\, \mathsf{P}$, P is negative, and $A^{\perp} = \forall\alpha_0\, \exists\alpha_1 \forall\alpha_2 \ldots \exists\alpha_{n-2} \forall\alpha_{n-1}\, \neg\mathsf{P}$

Figure 1 Term Assignment Rules for $\mathsf{IL} + \mathsf{EM}$

the free variables are a and those of A minus α. A term of the form $\mathtt{H}_a^{\forall\alpha A} m$, with $m \in \mathcal{L}$, is said to be *active*, if its only free variable is a: it represents a raise operator which has been turned on. The hypotheses for propositional formulas P of any form will be represented by terms $\mathtt{H}^{\mathsf{P}}$, regardless of their being introduced in the right or left premise of the excluded middle. Hence, the letter $\mathtt{H}$ stands for an hypothesis which does not "wait" for a witness, while $\mathtt{W}$ for one which does.

In our formulation, the excluded middle is restricted to negative propositional formulas, in the case of EM_0, and to prenex formulas with alternating quantifiers and whose propositional matrix is negative, in the case of EM_n. From the logical viewpoint, however, this is not at all a restriction, since we claim that any *arbitrary* instance $A \vee \neg A$ of the excluded middle can be proved in our system by standard, but tortuous, logical manipulations (see [1] for a proof). The fact that our system captures full classical first-order logic is not surprising, of course, since every formula is classically equivalent to a prenex one. From the computational viewpoint, in fact, we have directly modeled the most difficult cases of EM. It is quite clear that similar reduction rules for the less interesting cases of propositional connectives can be easily given, since $\wedge$ is just a finitary counterpart of $\forall$ and $\vee$ of $\exists$. For economy of presentation, we delay the treatment to future work.

In the following, we assume the usual renaming rules and alpha equivalences to avoid capture of variables in the reduction rules that we shall give. We also observe that every typed term which has been obtained by an elimination as a last rule, can be written as $r\,t_1\,t_2 \ldots t_n$ $(n \geq 0)$, where r is either a variable x or a term $\mathtt{H}_a^{\forall\alpha A}$ or $\mathtt{H}^{\mathsf{P}}$ or a redex and each t_i is either a term (when $r\,t_1\,\ldots t_i$ is obtained by an $\rightarrow$-elimination rule or by a $\forall$-elimination rule) or a constant π_i (when $r\,t_1\,\ldots t_i$ is obtained by an $\wedge$-elimination rule) or an expression $[x_0.u_0, x_1.u_1]$ (when $r\,t_1\,\ldots t_i$ is obtained by an $\vee$-elimination rule) or an expression $[(\alpha, x).u]$ (when $r\,t_1\,\ldots t_i$ is obtained by an $\exists$-elimination rule).

We are now going to explain the basic reduction rules for the proof terms of $\mathsf{IL} + \mathsf{EM}$, which are given in Figure 2. As usual, one has also the axiom scheme: $E[t] \mapsto E[u]$, whenever $t \mapsto u$ and for any context E. With $\mapsto^*$ we shall denote the reflexive and transitive closure of the one-step reduction $\mapsto$.

Reduction Rules for IL

$(\lambda x.u)t \mapsto u[t/x] \qquad (\lambda\alpha.u)t \mapsto u[t/\alpha]$

$\langle u_0, u_1\rangle\pi_i \mapsto u_i$, for i=0,1

$\iota_i(u)[x_1.t_1, x_2.t_2] \mapsto t_i[u/x_i]$, for i=0,1

$(n, u)[(\alpha, x).v] \mapsto v[n/\alpha][u/x]$, for each numeral n

Permutation Rules for EM_0

$(u \mid v)w \mapsto uw \mid vw$

$(u \mid v)\pi_i \mapsto u\pi_i \mid v\pi_i$

$(u \mid v)[x.w_1, y.w_2] \mapsto u[x.w_1, y.w_2] \mid v[x.w_1, y.w_2]$

$(u \mid v)[(\alpha, x).w] \mapsto u[(\alpha, x).w] \mid v[(\alpha, x).w]$

Permutation Rules for EM_n

$(u \blacktriangleright_a v)w \mapsto uw \blacktriangleright_a vw$, if a does not occur free in w

$(u \blacktriangleright_a v)\pi_i \mapsto u\pi_i \blacktriangleright_a v\pi_i$

$(u \blacktriangleright_a v)[x.w_1, y.w_2] \mapsto u[x.w_1, y.w_2] \blacktriangleright_a v[x.w_1, y.w_2]$, if a does not occur free in w_1, w_2

$(u \blacktriangleright_a v)[(\alpha, x).w] \mapsto u[(\alpha, x).w] \blacktriangleright_a v[(\alpha, x).w]$, if a does not occur free in w_1, w_2

Reduction Rules for EM_n

$u \blacktriangleright_a v \mapsto u$, if a does not occur free in u

$u \blacktriangleright\!|_a v \mapsto v[a := n] \blacktriangleright_b (u[a := n] \blacktriangleright\!|_a v)$, whenever u has some *active* subterm $\mathtt{H}_a^{\forall\alpha A}m$, $n = (m, b)$ and b is fresh

---

Figure 2 Reduction Rules for $\mathsf{IL} + \mathsf{EM}$

We find among them the ordinary reductions of intuitionistic logic for the logical con-

stants. Permutation Rules for EM_n are an instance of Prawitz's permutation rules for $\vee$-elimination [24]. The reduction rules for EM_n model the exception handling mechanism explained in Section §1. *Raising* an exception n in $u \,\mathbf{|}_a\, v$ removes some (actually, the *active* ones) occurrences of hypotheses $\mathtt{H}_a^{\forall\alpha A}$ in u and all occurrences of hypotheses $\mathtt{W}_a^{\exists\alpha P}$ in v, introducing simpler hypotheses; we define first an operation removing them, and denoted $v[a := n]$.

■ **Definition 2** (Exception Substitution)**.** Suppose v is any proof term and $n = (m, b)$, where m is a term of $\mathcal{L}$ and b an EM-hypothesis variable. Then:

1. If every free occurrence of a in v is of the form $\mathtt{W}_a^{\exists\alpha A}$, and $\exists\alpha\, A$ is prenex with alternating quantifiers, we define
$$v[a := n]$$
as the term obtained from v by replacing (without capture of b) each subterm $\mathtt{W}_a^{\exists\alpha A}$ corresponding to a free occurrence of a in v by $(m, \mathtt{H}_b^{A[m/\alpha]})$, if A is not propositional, by $(m, \mathtt{H}^{A[m/\alpha]})$ otherwise.
2. If every free occurrence of a in v is of the form $\mathtt{H}_a^{\forall\alpha A}$, and $\forall\alpha\, A$ is prenex with alternating quantifiers, we define
$$v[a := n]$$
as the term obtained from v by replacing (without capture of b) each subterm $\mathtt{H}_a^{\forall\alpha A} m$ corresponding to a free occurrence of a in v by $\mathtt{W}_b^{A[m/\alpha]}$, if A is not propositional, by $\mathtt{H}^{A[m/\alpha]}$ otherwise.

▶ Remark. In the second case of Definition 2 of $v[a := n]$, subterms of the form $\mathtt{H}_a^{\forall\alpha \mathsf{P}} m$, with P propositional, are replaced with $\mathtt{H}^{\mathsf{P}[m/\alpha]}$, because there is no exception and in particular no witness for $\mathsf{P}[m/\alpha]$ to be waited for and caught. Moreover, we remark that the substitution may replace only prenex hypotheses with alternating quantifiers, thus those introduced by the rule EM_n.

In the term $u \,|\, v$, the subterms u and v are forever divided and represent disjoint computational paths: communication between them is not even possible, because there is no associated exception mechanism. The rules for EM_n instead translate the informal idea of exception handling we sketched in the introduction:

1. The first EM_n-reduction: $u \,\mathbf{|}_a\, v \mapsto u$ (a does not occur free in u). This rule says that no free hypothesis of the shape $\mathtt{H}_a^{\forall\alpha A} : \forall\alpha A$ occurs in u and thus it is unnecessary in the proof and in the computation; consequently, the proof term $u \,\mathbf{|}_a\, v$ may be simplified to u and the computation carry on following only the reduction tree of u. In this case the exceptional part v of $u \,\mathbf{|}_a\, v$ is never used.
2. The second EM_n-reduction: $u \,\mathbf{\|}_a\, v \mapsto v[a := n] \,\mathbf{|}_b\, (u[a := n] \,\mathbf{\|}_a\, v)$ (where u has some active subterm $\mathtt{H}_a^{\forall\alpha A} m$ and $n = (m, b)$). This rule says that the "active" hypothesis $\mathtt{H}_a^{\forall\alpha A} m : A[m/\alpha]$, automatically raises in $u \,\mathbf{|}_a\, v$ the exception n. The raise of the exception (remember that it is related to the hypothesis variable a) has the following effects:
i) we perform the exception substitution $[a := n]$ in v (Definition 2). This means that we replace each occurrence of the term $\mathtt{W}_a^{\exists\alpha A^\perp}$ corresponding to a free occurrence of a in v by $(m, \mathtt{H}_b^{A^\perp[m/\alpha]})$ or $(m, \mathtt{H}^{A^\perp[m/\alpha]})$, according as to whether A is propositional or not. This way, we add the exceptional part $v[a := n]$ of $u \,\mathbf{\|}_a\, v$ to the computation as the left side of the sequence of bars $\mathbf{|}_b$. The new variable b, guaranteed to be "fresh" by definition, corresponds to the newly made hypothesis $A^\perp[m/\alpha]$ that ensures, in this "universe", that m is a correct witness for $\exists\alpha A^\perp$.

ii) on the right side of the $\|_b$ we have the term $(u[a := n] \|_a v)$ obtained from $u \|_a v$ by performing the substitution $[a := n]$ in u. The substitution removes all the occurrences of $\mathtt{H}_a^{\forall\alpha A} m$ in u, which are consumed by the raise of the correspondent exception n, and replace them with a new simpler hypothesis $\mathtt{W}_b^{A[m/\alpha]}$ (or $\mathtt{H}^{A[m/\alpha]}$), which confirms, in this "universe", the stronger $\forall\alpha A$. Notice that after the substitution $u[a := n]$ some free occurrence of a in u may still be there (the replaced occurrences of a are only the ones of the form $\mathtt{H}_a^{\forall\alpha A} m$); as a consequence, in the possible further reduction of the subterm $u[a := n] \|_a v$ an exception corresponding to the variable a may be raised again.
Notice that $\|_b$ is a strictly shorter sequence of bars with respect to the sequence $\|_a$; on the other hand, we also remark that the complexity of the formula $A[m/\alpha]$ is strictly lower with respect to the complexity of the hypothesis $\forall\alpha A$.

■ **Definition 3** (Normal Forms and Strongly Normalizable Terms)**.**

- A $\mapsto$-redex is a term u such that $u \mapsto v$ for some v and basic reduction of Figure 2. A term t is called an $\mapsto$-*normal* form (or simply *normal form*) if t does not contain as subterm any $\mapsto$-redex. We define NF to be the set of normal untyped proof terms.
- A sequence (finite or infinite) of proof terms $u_1, u_2, \ldots, u_n, \ldots$ is said to be a reduction of t, if $t = u_1$, and for all i, $u_i \mapsto u_{i+1}$. A proof term u of $\mathsf{IL} + \mathsf{EM}$ is *strongly normalizable* if there is no infinite reduction of u. We denote with SN the set of strongly normalizable terms of $\mathsf{IL} + \mathsf{EM}$.

Assume that Γ is a context, t an untyped proof term and A a formula, and $\Gamma \vdash t : A$: then t is said to be a typed proof term. Typing assignment satisfies Weakening, Exchange and Thinning, as usual. We claim that the reduction defined in Figure 2 satisfy the important Subject Reduction Theorem: reduction steps at the level of proof terms correspond to logically sound transformations at the level of proofs.

■ **Theorem 4** (Subject Reduction)**.**

If $\Gamma \vdash t : A$ and $t \mapsto u$ then $\Gamma \vdash t : A$.

Proof. The proof is by induction over t and is completely standard except for the EM_n reductions: we have sketched in the introduction how they should be typed. ◀

We now introduce the concept of quasi-closed term, which intuitively is a term behaving as a closed one, in the sense that it can be executed, but that contains some free simply universal hypotheses on which its correctness depends.

■ **Definition 5** (Quasi-Closed terms)**.**

1. An untyped proof term t is said to be *quasi-closed*, if it contains as free variables only hypothesis variables $a_1, \ldots, a_n$, such that each occurrence of them is of the form $\mathtt{H}_{a_i}^{\forall\vec{\alpha}\mathsf{P}_i}$, where $\forall\vec{\alpha}\,\mathsf{P}_i$ is simply universal.

The class of quasi-closed terms is meaningful from a computational viewpoint, as explained in Section 4.

3 The System $\mathsf{IL} + \mathsf{EM}^\star$: a Leap into Non-Determinism

The aim of this section is to prove that each well-typed term of $\mathsf{IL}+\mathsf{EM}$ is strongly normalizing. To this end, we make a pit stop into the magic world of non-determinism. The idea is to map $\mathsf{IL} + \mathsf{EM}$ to a carefully defined non-deterministic variant $\mathsf{IL} + \mathsf{EM}^\star$, for which strong

normalization is proven. The Strong Normalization Theorem for $\mathsf{IL}+\mathsf{EM}$ will plainly follow as a corollary. A similar proof technique, inspired to [8], an update of [6].

We now introduce the non-deterministic system $\mathsf{IL}+\mathsf{EM}^\star$, which is still a standard natural deduction system for intuitionistic first-order logic with excluded middle. The only syntactical difference with the system $\mathsf{IL}+\mathsf{EM}$ lies in the shape of proof terms, and is really tiny: the proof terms for EM and EM-hypotheses lose the hypothesis variables used to name them. Thus the grammar of untyped proof terms of $\mathsf{IL}+\mathsf{EM}^\star$ is defined to be the following:

Grammar of Untyped Terms of $\mathsf{IL}+\mathsf{EM}^\star$

$$t,u,v ::= x \mid tu \mid tm \mid \lambda x\, u \mid \lambda\alpha\, u \mid \langle t,u\rangle \mid u\,\pi_0 \mid u\,\pi_1 \mid \iota_0(u) \mid \iota_1(u) \mid t[x.u, y.v] \mid (m,t) \mid t[(\alpha,x).u]$$
$$\mid (u \underbrace{\mid\mid \ldots \mid}_{n+1 \text{ bars}} v) \mid \mathtt{H}^{\forall\alpha A} \mid \mathtt{W}^{\exists\alpha A}$$

where m ranges over terms of $\mathcal{L}$, x over proof terms variables and A is either prenex with alternating quantifiers or simply universal.

The term assignment rules of $\mathsf{IL}+\mathsf{EM}^\star$ are exactly the same of $\mathsf{IL}+\mathsf{EM}$, but for the ones for EM-hypotheses and EM, which just replace hypothesis variables a from the former proof terms:

Axioms $\quad \Gamma, a:\forall\alpha A \vdash \mathtt{H}^{\forall\alpha A} : \forall\alpha A \qquad \Gamma, a:\exists\alpha A \vdash \mathtt{W}^{\exists\alpha A} : \exists\alpha A$

$$\mathsf{EM}^\star{}_n \quad \frac{\Gamma, a:\forall\alpha A \vdash w_1 : C \quad \Gamma, a:\exists\alpha A^\perp \vdash w_2 : C}{\Gamma \vdash w_1 \underbrace{\mid\mid \ldots \mid}_{n+1} w_2 : C}$$

The reduction rules for the terms of $\mathsf{IL}+\mathsf{EM}^\star$ are defined in Figure 3 and are those of the first two groups for $\mathsf{IL}+\mathsf{EM}_1$, plus new non-deterministic rules for $\mathsf{EM}^\star$ and closure by context (with $\rightsquigarrow^*$ we shall denote the reflexive and transitive closure of the one-step reduction $\rightsquigarrow$).

We explain now the non-deterministic part of the reduction rules. The reduction rule for $\mathtt{H}^{\forall\alpha A}$ says that, when the constant is active (i.e. applied to a closed term $m \in \mathcal{L}$ and $\forall\alpha A$ is closed) it is possible to replace an universal hypothesis $\forall\alpha A$ with an hypothesis $A[m/\alpha]$, denoted by the constant $\mathtt{W}^{A[m/\alpha]}$, when $A[m/\alpha]$ is not propositional and thus of the shape $\exists\beta B$ for some variable β and some universal formula B. The intuition behind the reduction rule for $\mathtt{W}^{\exists\alpha A}$ is the following: the term $\mathtt{W}^{\exists\alpha A}$ behaves as a "search" operator, which spans non-deterministically all first-order terms as possible witnesses of $\exists\alpha A^\perp$ and makes the hypothesis that they are correct (these branches correspond to all the possible pairs $(m, \mathtt{H}^{A[m/\alpha]})$). The first two rules for the operator $\mid$ are standard reductions for the non deterministic choice operator (see [14, 13]). The third rule, in joint with the reductions for $\mathtt{H}^{\forall\alpha A}$ and $\mathtt{W}^{\exists\alpha A}$, is able to "simulate" the reductions of the deterministic $u \mid_a v$ and, in particular, the exception substitution mechanism $[a := n]$.

In the following, we define $\mathsf{SN}^\star$ to be the set of strongly normalizing proof terms with respect to the non-deterministic reduction $\rightsquigarrow$. The reduction tree of a strongly normalizable term with respect to $\rightsquigarrow$ is no more finite, but still well-founded. It is well-known that it

is possible to assign to each node of a well-founded tree an ordinal number, in such a way it decreases passing from a node to any of its sons. We will call the *ordinal size* of a term $t \in \mathsf{SN}^\star$ the ordinal number assigned to the root of its reduction tree and we denote it by $h(t)$; thus, if $t \rightsquigarrow u$, then $h(t) > h(u)$. To fix ideas, one may define $h(t) := \mathsf{sup}\{h(u) + 1 \mid t \mapsto u\}$.

Reduction Rules for IL

$(\lambda x.u)t \rightsquigarrow u[t/x] \qquad (\lambda\alpha.u)t \rightsquigarrow u[t/\alpha]$

$\pi_i\langle u_0, u_1\rangle \rightsquigarrow u_i$, for $i = 0, 1$

$\iota_i(u)[x_1.t_1, x_2.t_2] \rightsquigarrow t_i[u/x_i]$, for $i = 0, 1$

$(n, u)[(\alpha, x).v] \rightsquigarrow v[n/\alpha][u/x]$, for each numeral n

Permutation Rules for EM*

$(u \blacktriangleright v)w \rightsquigarrow uw \blacktriangleright vw$

$(u \blacktriangleright v)\pi_i \rightsquigarrow u\pi_i \blacktriangleright v\pi_i$

$(u \blacktriangleright v)[x.w_1, y.w_2] \rightsquigarrow u[x.w_1, y.w_2] \blacktriangleright v[x.w_1, y.w_2]$

$(u \blacktriangleright v)[(\alpha, x).w] \rightsquigarrow u[(\alpha, x).w] \blacktriangleright v[(\alpha, x).w]$

Reduction Rules for EM*

$(\mathtt{H}^{\forall\alpha A})m \rightsquigarrow \mathtt{W}^{A[m/\alpha]}$, for every closed term m of $\mathcal{L}$ and existential A

$(\mathtt{H}^{\forall\alpha \mathsf{P}})m \rightsquigarrow \mathtt{H}^{\mathsf{P}[m/\alpha]}$, for every closed term m of $\mathcal{L}$

$\mathtt{W}^{\exists\alpha A} \rightsquigarrow (m, \mathtt{H}^{A[m/\alpha]})$, for every closed term m of $\mathcal{L}$

$u \blacktriangleright v \rightsquigarrow u$

$u \blacktriangleright v \rightsquigarrow v$

$u \blacktriangleright\!\blacktriangleright v \rightsquigarrow v \blacktriangleright (u^- \blacktriangleright\!\blacktriangleright v)$

where u^- is the term obtained from u by replacing some occurrences of a subterm $(\mathtt{H}^{\forall\alpha A})m$ with $\mathtt{W}^{A[m/\alpha]}$ (or with $\mathtt{H}^{A[m/\alpha]}$ when A is not existential)

Figure 3 Reduction Rules for IL + EM*

We now define the obvious translation mapping untyped proof terms of IL + EM into untyped terms of IL + EM*, which just erases every occurrence of every EM-hypothesis variable a.

Definition 6 (Translation of untyped proof terms of IL + EM into IL + EM*)**.** We define a translation $\_^*$ mapping untyped proof terms of IL + EM into untyped proof terms of IL + EM*: t^* is defined as the term of IL + EM* obtained from t by erasing every EM hypothesis variable a.

We now show that the reduction relation $\rightsquigarrow$ for the proof terms of IL + EM* can easily simulate the reduction relation $\mapsto$ for the terms of IL + EM. This is trivial for the proper reductions of IL and the permutative reductions for EM, while the reduction rules for the terms of the form $u \blacktriangleright_a v$ can be plainly simulated by $\rightsquigarrow$ with non-deterministic guesses. In particular, each reduction step between terms of IL + EM corresponds to *at least* a step between their translations:

Proposition 7 (Preservation of the Reduction Relation $\mapsto$ by $\rightsquigarrow$)**.** *Let v be any untyped proof term of* IL + EM*. Then $v \mapsto w \implies v^* \rightsquigarrow^+ w^*$*

Proof. It is sufficient to prove the proposition when v is a redex r. We have several possibilities, almost all trivial, and we choose only some representative cases:

1. $r = (\lambda x\, u)t \mapsto u[t/x]$. We verify indeed that

$$((\lambda x\, u)t)^* = (\lambda x\, u^*)t^* \rightsquigarrow u^*[t^*/x] = u[t/x]^*$$

2. $r = (u \parallel v)w \mapsto uw \parallel vw$. We verify indeed that

$$((u \parallel v)w)^* = (u^* \parallel v^*)w^* \rightsquigarrow u^*w^* \parallel v^*w^* \rightsquigarrow (uw \parallel vw)^*$$

3. $r = u \parallel_a v \mapsto v[a := n] \parallel_b (u[a := n] \parallel_a v)$ (where u has some active subterm $\mathtt{H}_a^{\forall\alpha A} m$ and $n = (m, b)$).
We verify indeed – by choosing the appropriate reduction rule for $\parallel$ and applying the $\mathsf{EM}^\star$ reduction rules $(\mathtt{H}^{\forall\alpha A})m \rightsquigarrow \mathtt{W}^{A[m/\alpha]}$ (or $(\mathtt{H}^{\forall\alpha \mathsf{P}})m \rightsquigarrow \mathtt{H}^{\mathsf{P}[m/\alpha]}$) and $\mathtt{W}^{\exists\alpha A} \rightsquigarrow (m, \mathtt{H}^{A[m/\alpha]})$ – that

$$\begin{aligned}(u \parallel_a v)^* &= u^* \parallel v^* \rightsquigarrow v^* \parallel ((u^*)^- \parallel v^*)\\ &\rightsquigarrow^* (v[a := n])^* \parallel ((u[a := n])^* \parallel v^*)\\ &\rightsquigarrow^* (v[a := n] \parallel_b (u[a := n] \parallel_a v))^*\end{aligned}$$

(where u^- is the term obtained from u^* by replacing some occurrences of a subterm $(\mathtt{H}^{\forall\alpha A})m$ with $\mathtt{W}^{A[m/\alpha]}$ or $\mathtt{H}^{A[m/\alpha]}$ when A is propositional)

3.1 Reducibility

We now want to prove the strong normalization theorem for $\mathsf{IL} + \mathsf{EM}^\star$: every term t which is typed in $\mathsf{IL} + \mathsf{EM}^\star$ is strongly normalizable. We use a simple extension of the reducibility method of Tait-Girard [15].

■ **Definition 8** (Reducibility)**.** Assume t is a term in the grammar of untyped terms of $\mathsf{IL} + \mathsf{EM}^\star$ and C is a formula of $\mathcal{L}$. We define the relation $t \mathsf{r} C$ ("t is reducible of type C") by induction and by cases according to the form of C:

1. $t \mathsf{r} \mathsf{P}$ if and only if $t \in \mathsf{SN}^\star$

2. $t \mathsf{r} A \wedge B$ if and only if $t\,\pi_0 \mathsf{r} A$ and $t\,\pi_1 \mathsf{r} B$

3. $t \mathsf{r} A \to B$ if and only if for all u, if $u \mathsf{r} A$, then $tu \mathsf{r} B$

4. $t \mathsf{r} A \vee B$ if and only if $t \in \mathsf{SN}^\star$ and $t \rightsquigarrow^* \iota_0(u)$ implies $u \mathsf{r} A$ and $t \rightsquigarrow^* \iota_1(u)$ implies $u \mathsf{r} B$

5. $t \mathsf{r} \forall\alpha A$ if and only if for every term m of $\mathcal{L}$, $tm \mathsf{r} A[m/\alpha]$

6. $t \mathsf{r} \exists\alpha A$ if and only if $t \in \mathsf{SN}^\star$ and for every term m of $\mathcal{L}$, if $t \rightsquigarrow^* (m, u)$, then $u \mathsf{r} A[m/\alpha]$

3.2 Properties of Reducible Terms

In this section we prove that the set of reducible terms for a given formula C satisfies the usual properties of a Girard reducibility candidate.

Following [15], neutral terms are terms that are not "values" and need to be further computed.

■ **Definition 9** (Neutrality)**.** A proof term is neutral if it is not of the form $\lambda x\, u$ or $\lambda\alpha\, u$ or $\langle u, t\rangle$ or $\iota_i(u)$ or (t, u) or $u \parallel v$ or $\mathtt{H}^{\forall\alpha A}$.

■ **Definition 10** (Reducibility Candidates)**.** Extending the approach of [15], we define four properties **(CR1)**, **(CR2)**, **(CR3)**, **(CR4)** of reducible terms t:

(CR1) If $t \mathsf{r} A$, then $t \in \mathsf{SN}^\star$.

(CR2) If $t \mathsf{r} A$ and $t \rightsquigarrow^* t'$, then $t' \mathsf{r} A$.

(CR3) If t is neutral and for every t', $t \rightsquigarrow t'$ implies $t' \mathsf{r} A$, then $t \mathsf{r} A$.

(CR4) $t = u \mid v \mathsf{r} A$ if and only if $u \mathsf{r} A$ and $v \mathsf{r} A$.

We now prove, as usual, that every term t possesses the reducibility candidate properties. The arguments for establishing **(CR1)**, **(CR2)**, **(CR3)**, are in many cases standard (see [15]).

■ **Proposition 11.** *Let t be a term of $\mathsf{IL} + \mathsf{EM}^\star$. Then t has the properties **(CR1)**, **(CR2)**, **(CR3)**, **(CR4)**.*

Proof. By induction on C.

- C is atomic. Then $t \mathsf{r} C$ means $t \in \mathsf{SN}^\star$. Therefore **(CR1)**, **(CR2)**, **(CR3)** are trivial.
  (CR4). Suppose $u, v \mathsf{r} C$. Then, by definition, $u \in \mathsf{SN}^\star$, $v \in \mathsf{SN}^\star$. We have to show that $u \parallel v \in \mathsf{SN}^\star$. We proceed by triple induction on the number of bars in $\parallel$ and the ordinal heights of the reduction trees of u, v. We show that $u \parallel v \rightsquigarrow z$ implies $z \in \mathsf{SN}^\star$. If $z = u$ or $z = v$ the thesis is trivial. If $z = u' \parallel v$ or $z = u \parallel v'$, by induction hypothesis, $z \in \mathsf{SN}^\star$. If $z = v \mid (u^- \parallel v)$, where u^- is the term obtained from u by replacing some occurrences of a subterm $(\mathtt{H}^{\forall \alpha A})m$ with $\mathtt{W}^{A[m/\alpha]}$ (or $\mathtt{H}^{A[m/\alpha]}$), then $u \rightsquigarrow u^-$, therefore by induction hypothesis $(u^- \parallel v) \in \mathsf{SN}^\star$; we conclude, again by induction hypothesis, that $z \in \mathsf{SN}^\star$.

- $C = A \to B$.

  (CR1). Suppose $t \mathsf{r} A \to B$. By induction hypothesis **(CR3)**, for any variable x, we have $x \mathsf{r} A$. Therefore, $tx \mathsf{r} B$, and by **(CR1)**, $tx \in \mathsf{SN}^\star$, and thus $t \in \mathsf{SN}^\star$.

  (CR2). Suppose $t \mathsf{r} A \to B$ and $t \rightsquigarrow t'$. Let $u \mathsf{r} A$: we have to show $t'u \mathsf{r} B$. Since $tu \mathsf{r} B$ and $tu \rightsquigarrow t'u$, we have by the induction hypothesis **(CR2)** that $t'u \mathsf{r} B$.

  (CR3). Assume t is neutral and $t \rightsquigarrow t'$ implies $t' \mathsf{r} A \to B$. Suppose $u \mathsf{r} A$; we have to show that $tu \mathsf{r} B$. We proceed by induction on the ordinal height of the reduction tree of u ($u \in \mathsf{SN}^\star$ by induction hypothesis **(CR1)**). By induction hypothesis, **(CR3)** holds for the type B. So assume $tu \rightsquigarrow z$; it is enough to show that $z \mathsf{r} B$. If $z = t'u$, with $t \rightsquigarrow t'$, then by hypothesis $t' \mathsf{r} A \to B$, so $z \mathsf{r} B$. If $z = tu'$, with $u \rightsquigarrow u'$, by induction hypothesis **(CR2)** $u' \mathsf{r} A$, and therefore $z \mathsf{r} B$ by the induction hypothesis relative to the size of the reduction tree of u'. There are no other cases since t is neutral.

  (CR4). $\Rightarrow$). Suppose $t = u \mid v \mathsf{r} A \to B$. Since $t \rightsquigarrow u$, $t \rightsquigarrow v$, by **(CR2)**, $u \mathsf{r} A \to B$ and $v \mathsf{r} A \to B$.
  $\Leftarrow$). Suppose $u \mathsf{r} A \to B$ and $v \mathsf{r} A \to B$. Let $w \mathsf{r} A$. We show by quadruple induction on the number of bars in $\mid$, the ordinal heights of the reduction trees of u, v, w (they are all in $\mathsf{SN}^\star$ by **(CR1)**) that $(u \parallel v)w \mathsf{r} B$. By induction hypothesis **(CR3)**, it is enough to

assume $(u \parallel v)w \rightsquigarrow z$ and show $z \mathsf{r} B$. If $z = uw$ or vw, we are done. If $z = (u' \parallel v)w$ or $z = (u \parallel v')w$ or $(u \parallel v)w'$, with $u \rightsquigarrow u'$, $v \rightsquigarrow v'$ and $w \rightsquigarrow w'$, we obtain $z \mathsf{r} B$ by **(CR2)** and induction hypothesis. If $z = (uw \parallel vw)$, by induction hypothesis **(CR4)**, $z \mathsf{r} B$.
If $z = (v \mid (u^- \parallel v))w$, where u^- is the term obtained from u by replacing some occurrences of a subterm $(\mathtt{H}^{\forall\alpha A})m$ with $\mathtt{W}^{A[m/\alpha]}$ (or $\mathtt{H}^{A[m/\alpha]}$), then $u \rightsquigarrow u^-$, therefore by **(CR2)** and induction hypothesis, for all $r \mathsf{r} A$, we have $(u^- \parallel v)r \mathsf{r} B$ and thus $(u^- \parallel v) \mathsf{r} A \to B$. We conclude by induction hypothesis that $v \mid (u^- \parallel v) \mathsf{r} A \to B$ and thus $z \mathsf{r} B$.

- $C = \forall\alpha A$ or $C = A \wedge B$. Similar to the case $C = A \to B$.

- $C = A_0 \vee A_1$.

  (CR1) is trivial.

  (CR2). Suppose $t \mathsf{r} A_0 \vee A_1$ and $t \rightsquigarrow^* t'$. Then $t' \in \mathsf{SN}^\star$, since $t \in \mathsf{SN}^\star$. Moreover, suppose $t' \rightsquigarrow^* \iota_i(u)$. Then also $t \rightsquigarrow^* \iota_i(u)$, so $u \mathsf{r} A_i$.

  (CR3). Assume t is neutral and $t \rightsquigarrow t'$ implies $t' \mathsf{r} A_0 \vee A_1$. Since $t \rightsquigarrow t'$ implies $t' \in \mathsf{SN}^\star$, we have $t \in \mathsf{SN}^\star$. Moreover, if $t \rightsquigarrow^* \iota_i(u)$, then, since t is neutral, $t \rightsquigarrow t' \rightsquigarrow^* \iota_i(u)$ and thus $u \mathsf{r} A_i$.

  (CR4). $\Rightarrow$). Suppose $t = u \mid v \mathsf{r} A_0 \vee A_1$. Since $t \rightsquigarrow u$, $t \rightsquigarrow v$, by **(CR2)**, $u \mathsf{r} A_0 \vee A_1$ and $v \mathsf{r} A_0 \vee A_1$.
  $\Leftarrow$). Suppose $u \mathsf{r} A_0 \vee A_1$ and $v \mathsf{r} A_0 \vee A_1$. We have to show that $u \parallel v \mathsf{r} A_0 \vee A_1$. By **(CR1)**, $u, v \in \mathsf{SN}^\star$; therefore, as shown in the case $C = P$, $u \parallel v \in \mathsf{SN}^\star$. Moreover, suppose $u \parallel v \rightsquigarrow^* \iota_i(w)$. It is enough to show that either $u \rightsquigarrow^* \iota_i(w)$ or $v \rightsquigarrow^* \iota_i(w)$; this implies $w \mathsf{r} A_i$, and we are done. We proceed by triple induction on the number of bars in $\parallel$ and the ordinal heights of the reduction trees of u, v. Let us consider the first reduction step: $u \parallel v \rightsquigarrow z \rightsquigarrow^* \iota_i(w)$. If $z = u$ or $z = v$, we are done. If $z = u' \parallel v$ or $z = u \parallel v'$, with $u \rightsquigarrow u'$ and $v \rightsquigarrow v'$, we obtain $u \rightsquigarrow^* \iota_i(w)$ or $v \rightsquigarrow^* \iota_i(w)$ by induction hypothesis applied to z. If $z = v \mid (u^- \parallel v)$, where u^- is the term obtained from u by replacing some occurrences of a subterm $(\mathtt{H}^{\forall\alpha A})m$ with $\mathtt{W}^{A[m/\alpha]}$ (or $\mathtt{H}^{A[m/\alpha]}$), then $u \rightsquigarrow u^-$. Therefore, by induction hypothesis applied to z, either $v \rightsquigarrow^* \iota_i(w)$ or $u^- \parallel v \rightsquigarrow^* \iota_i(w)$. In the first case, we are done; in the second, by induction hypothesis applied to $u^- \parallel v$, we obtain either $u \rightsquigarrow u^- \rightsquigarrow^* \iota_i(w)$ or $v \rightsquigarrow^* \iota_i(w)$, which completes the proof.

- $C = \exists\alpha^{\mathtt{N}} A$. Similar to the case $t = A_0 \vee A_1$.

The next task is to prove that all introduction and elimination rules of $\mathsf{IL} + \mathsf{EM}^\star$ define a reducible term from a list of reducible terms for all premises (Adequacy Theorem 13). In some case that is true by definition of reducibility; we list below some non-trivial but standard cases we have to prove.

Proposition 12.

1. *If for every $t \mathsf{r} A$, $u[t/x] \mathsf{r} B$, then $\lambda x\, u \mathsf{r} A \to B$.*
2. *If for every term m of $\mathcal{L}$, $u[m/\alpha] \mathsf{r} B[m/\alpha]$, then $\lambda\alpha\, u \mathsf{r} \forall\alpha B$.*
3. *If $u \mathsf{r} A_0$ and $v \mathsf{r} A_1$, then $\langle u, v\rangle\pi_i \mathsf{r} A_i$.*
4. *If $t \mathsf{r} A_0 \vee A_1$ and for every $t_i \mathsf{r} A_i$ it holds $u_i[t_i/x_i] \mathsf{r} C$, then $t[x_0.u_0, x_1.u_1] \mathsf{r} C$.*
5. *If $t \mathsf{r} \exists\alpha A$ and for every term m of $\mathcal{L}$ and $v \mathsf{r} A[m/\alpha]$ it holds $u[m/\alpha][v/x] \mathsf{r} C$, then $t[(\alpha, x).u] \mathsf{r} C$.*

Proof.

1. As in [15].

2. As 1.

3. As in [15].

4. Suppose $t \mathsf{r} A_0 \vee A_1$ and for every $t_i \mathsf{r} A_i$ it holds $u_i[t_i/x_i] \mathsf{r} C$. We observe that by **(CR3)**, $x_i \mathsf{r} A_i$, and so we have $u_i \mathsf{r} A_i$. Thus, in order to prove $t[x_0.u_0, x_1.u_1] \mathsf{r} C$, by **(CR1)**, we can reason by triple induction on the ordinal sizes of the reduction trees of t, u_0, u_1. By **(CR3)**, it suffices to show that $t[x_0.u_0, x_1.u_1] \rightsquigarrow z$ implies $z \mathsf{r} C$. If $z = t'[x_0.u_0, x_1.u_1]$ or $z = t[x_0.u_0', x_1.u_1]$ or $z = t[x_0.u_0, x_1.u_1']$, with $t \rightsquigarrow t'$ and $u_i \rightsquigarrow u_i'$, then by **(CR2)** and by induction hypothesis $z \mathsf{r} C$. If $t = \iota_i(t_i)$ and $z = u_i[t_i/x_i]$, then $t_i \mathsf{r} A_i$; therefore, $z \mathsf{r} C$. If $t = w_0 \mid w_1$ and

$$z = (w_0[x_0.u_0, x_1.u_1]) \mid (w_1[x_0.u_0, x_1.u_1])$$

then, since $t = w_0 \mid w_1 \rightsquigarrow w_i$, by induction hypothesis $w_i[x_0.u_0, x_1.u_1] \mathsf{r} C$ for $i = 0, 1$. By **(CR4)**, we conclude $z \mathsf{r} C$.

5. Similar to 4.

3.3 The Adequacy Theorem

■ **Theorem 13** (Adequacy Theorem)**.** *Suppose that* $\Gamma \vdash w : A$ *in the system* $\mathsf{IL} + \mathsf{EM}^\star$*, with* $\Gamma = x_1 : A_1, \ldots, x_n : A_n, \Delta$ *(*Δ *not containing declarations of proof-term variables), and that the free variables of the formulas occurring in* Γ *and* A *are among* $\alpha_1, \ldots, \alpha_k$*. For all terms* $r_1, \ldots, r_k$ *of* $\mathcal{L}$*, if there are terms* $t_1, \ldots, t_n$ *such that*

for $i = 1, \ldots, n$, $t_i \mathsf{r} A_i[r_1/\alpha_1 \cdots r_k/\alpha_k]$

then

$w[t_1/x_1 \cdots t_n/x_n \ r_1/\alpha_1 \cdots r_k/\alpha_k] \mathsf{r} A[r_1/\alpha_1 \cdots r_k/\alpha_k]$

Proof.
Notation: for any term v and formula B, we denote

$v[t_1/x_1 \cdots t_n/x_n \ r_1/\alpha_1 \cdots r_k/\alpha_k]$

with $\overline{v}$ and

$B[r_1/\alpha_1 \cdots r_k/\alpha_k]$

with $\overline{B}$. We proceed by induction on w and cover only the case not already treated in [15]. Consider the last rule r in the derivation of $\Gamma \vdash w : A$:

1. We prove simultaneously the cases $\mathsf{r} = \Gamma \vdash \mathtt{W}^{\exists\alpha B} : \exists\alpha B$ and $\mathsf{r} = \Gamma \vdash \mathtt{H}^{\forall\alpha B}$ i.e. we want to prove that $\overline{w} = \overline{\mathtt{W}^{\exists\alpha B}} = \mathtt{W}^{\exists\alpha\overline{B}} \mathsf{r} \exists\alpha\overline{B} = \overline{A}$ and $\overline{w} = \overline{\mathtt{H}^{\forall\alpha B}} = \mathtt{H}^{\forall\alpha\overline{B}} \mathsf{r} \forall\alpha\overline{B} = \overline{A}$ respectively. We proceed by induction on B. Let us consider the terms $\overline{w} = \mathtt{W}^{\exists\alpha\overline{B}}$: we have that, for all term z such that $\mathtt{W}^{\exists\alpha\overline{B}} \rightsquigarrow z$, $z = (m, \mathtt{H}^{\overline{B}[m/\alpha]})$ for some $m \in \mathcal{L}$. It is possible to apply the induction hypothesis on $\mathtt{H}^{\overline{B}[m/\alpha]}$: thus $\mathtt{H}^{\overline{B}[m/\alpha]} \mathsf{r} \overline{B}[m/\alpha]$ holds and we can conclude $\mathtt{W}^{\exists\alpha\overline{B}} \mathsf{r} \exists\alpha\overline{B}$ by Definition 8.

Now, let us apply $\mathtt{H}^{\forall\alpha\overline{B}}$ to an arbitrary term $m \in \mathcal{L}$. Since $\mathtt{H}^{\forall\alpha\overline{B}}m \rightsquigarrow \mathtt{W}^{\overline{B}[m/\alpha]}$ or $\mathtt{H}^{\forall\alpha\overline{B}}m \rightsquigarrow \mathtt{H}^{\overline{B}[m/\alpha]}$ and by induction hypothesis $\mathtt{H}^{\overline{B}[m/\alpha]}, \mathtt{W}^{\overline{B}[m/\alpha]}$ r $\overline{B}[m/\alpha]$, we can conclude by **(CR3)**that $\mathtt{H}^{\forall\alpha\overline{B}}m$ r $\overline{B}[m/\alpha]$.

2. If r is a $\vee I$ rule, say left (the other case is symmetric), then $w = \iota_0(u)$, $A = B \vee C$ and $\Gamma \vdash u : B$. So, $\overline{w} = \iota_0(\overline{u})$. By induction hypothesis $\overline{u}$ r $\overline{B}$. Hence, $\overline{u} \in \mathsf{SN}^\star$. Moreover, suppose $\iota_0(\overline{u}) \rightsquigarrow^* \iota_0(v)$. Then $\overline{u} \rightsquigarrow^* v$ and thus by **(CR2)** v r $\overline{B}$. We conclude $\iota_0(\overline{u})$ r $\overline{B} \vee \overline{C} = \overline{A}$.

3. If r is is a $\vee E$ rule, then

$$w = u[x.w_1, y.w_2]$$

and $\Gamma \vdash u : B \vee C$, $\Gamma, x : B \vdash w_1 : D$, $\Gamma, y : C \vdash w_2 : D$, $A = D$. By induction hypothesis, we have $\overline{u}$ r $\overline{B} \vee \overline{C}$; moreover, for every t r $\overline{B}$, we have $\overline{w}_1[t/x]$ r $\overline{B}$ and for every t r $\overline{C}$, we have $\overline{w}_2[t/y]$ r $\overline{C}$. By proposition 12, we obtain $\overline{w} = \overline{u}[x.\overline{w}_1, y.\overline{w}_2]$ r $\overline{C}$

4. The cases $\mathsf{r} = \exists I$ and $\mathsf{r} = \exists E$ are similar respectively to $\vee I$ and $\vee E$.

5. If r is the $\forall E$ rule, then $w = ut$, $A = B[t/\alpha]$ and $\Gamma \vdash u : \forall\alpha B$. So, $\overline{w} = \overline{u}\overline{t}$. By inductive hypothesis $\overline{u}$ r $\forall\alpha\overline{B}$ and so $\overline{u}\overline{t}$ r $\overline{B}[\overline{t}/\alpha]$.

6. If r is the $\forall I$ rule, then $w = \lambda\alpha u$, $A = \forall\alpha B$ and $\Gamma \vdash u : B$ (with α not occurring free in the formulas of Γ). So, $\overline{w} = \lambda\alpha\overline{u}$, since we may assume $\alpha \neq \alpha_1, \ldots, \alpha_k$. Let t be a term of $\mathcal{L}$; by proposition 12), it is enough to prove that $\overline{u}[t/\alpha]$ r $\overline{B}[t/\alpha]$, which amounts to show that the induction hypothesis can be applied to u. For this purpose, we observe that, since $\alpha \neq \alpha_1, \ldots, \alpha_k$, for $i = 1, \ldots, n$ we have

$$t_i \ \mathsf{r} \ \overline{A}_i = \overline{A}_i[t/\alpha]$$

7. If it is the $\mathsf{EM}^\star$ rule, then $w = u \mid v$, $\Gamma, a : \forall\alpha B \vdash u : C$ and $\Gamma, a : \exists\alpha B^\perp \vdash v : C$ and $A = C$. By induction hypothesis, $\overline{u}, \overline{v}$ r $\overline{C}$. By **(CR4)**, we conclude $\overline{w} = (\overline{u} \mid \overline{v})$ r $\overline{C}$.

3.4 Strong Normalization of $\mathsf{IL} + \mathsf{EM}^\star$ and $\mathsf{IL} + \mathsf{EM}$

As corollary, one obtains strong normalization for $\mathsf{IL} + \mathsf{EM}^\star$.

■ **Corollary 14** (Strong Normalization for $\mathsf{IL} + \mathsf{EM}^\star$)**.** *Suppose* $\Gamma \vdash t : A$ *in* $\mathsf{IL} + \mathsf{EM}^\star$*. Then* $t \in \mathsf{SN}^\star$*.*

Proof. Assume $\Gamma = x_1 : A_1, \ldots, x_n : A_n, \Delta$ (Δ not containing declarations of proof-term variables). By **(CR1)**, one has x_i r A_i, for $i = 1, \ldots, n$. From Theorem 13, we derive that t r A. From **(CR1)**, we conclude that $t \in \mathsf{SN}^\star$.

The strong normalization of $\mathsf{IL} + \mathsf{EM}^\star$ is readily turned into a strong normalization result for $\mathsf{IL} + \mathsf{EM}$, since the reduction $\mapsto$ can be simulated by $\rightsquigarrow$.

■ **Corollary 15** (Strong Normalization for $\mathsf{IL} + \mathsf{EM}$)**.** *Suppose* $\Gamma \vdash t : A$ *in* $\mathsf{IL} + \mathsf{EM}$*. Then* $t \in \mathsf{SN}$*.*

Proof. By Proposition 7, any infinite reduction $t = t_1 \mapsto t_2 \mapsto \ldots \mapsto t_n \mapsto \ldots$ in $\mathsf{IL} + \mathsf{EM}$ gives rise to an infinite reduction $t^* = t_1^* \rightsquigarrow^+ t_2^* \rightsquigarrow^+ \ldots \rightsquigarrow^+ t_n^* \rightsquigarrow^+ \ldots$ in $\mathsf{IL} + \mathsf{EM}^\star$. By the strong normalization Corollary 15 for $\mathsf{IL} + \mathsf{EM}^\star$ and since clearly $\Gamma \vdash t^* : A$, infinite reductions of the latter kind cannot occur; thus neither of the former.

4 Back to $\mathsf{IL} + \mathsf{EM}$: Normal Form Property and Herbrand's Disjunction Extraction

In this section, we finally show that our exception-based Curry-Howard correspondence for classical logic is meaningful from the computational perspective. That is, not only every execution of every program we extract always terminates, but in the case of simply existential formulas $\exists\alpha\,\mathsf{P}$, any closed program of that type produces a complete finite sequence $m_1, m_2, \ldots, m_k$ of possible witnesses for $\exists\alpha\,\mathsf{P}$. This means that whatever first-order model we consider, there will be an i such that $\mathsf{P}[m_i/\alpha]$ is true in it. The result still holds whenever the program t is quasi-closed, which is to say, whenever $\exists\alpha\,\mathsf{P}$ is proven by means of a simply universal theory:

$$a_1 : \forall\vec{\alpha}\,\mathsf{P}_1, \ldots, a_n : \forall\vec{\alpha}\,\mathsf{P}_n \vdash t : \exists\alpha\,\mathsf{P}$$

In this case, for any first-order model of the formulas $a_1 : \forall\vec{\alpha}\,\mathsf{P}_1, \ldots, a_n : \forall\vec{\alpha}\mathsf{P}_n$, there will be an i such that $\mathsf{P}[m_i/\alpha]$ is true in it. Furthermore, by Subject Reduction, t will contain also a correctness certificate, in the sense that in the normal form of t one finds a proof-term for the formula $\mathsf{P}[m_1/\alpha] \vee \cdots \vee \mathsf{P}[m_k/\alpha]$. In other terms, we have provided a new proof and a new Curry-Howard computational interpretation of Herbrand's Theorem. The fact that we consider as hypotheses only simply universal ones, i.e. universal formulas without occurrences of $\vee$, is by no means restrictive: by EM_0, one can easily prove any propositional formula to be equivalent to a negative one, and thus to derive the former from the latter.

In order to prove our results, we first carry out a simple inspection of the normal forms of the terms having propositional or simply existential type. The crucial observation is that every such term contains an exception ready to be raised: more precisely, it has a active subterm of the form $\mathtt{H}_a^{\forall\alpha A} m$, for some $m \in \mathcal{L}$. From the logical point of view, this means that when one proves a formula of minimal complexity by means of a universal theory, one must use actively one of the universal hypotheses and obtain some concrete consequence of it. Such statements in first-order logic are typically drawn as consequences of the Subformula Property, but a much more primitive argument suffices here. This is indeed providential, since without permutation rules for $\vee$ and $\exists$, there will be no Subformula Property. Of course, we *do* have some permutation rules, namely those for the excluded middle: what is remarkable is that they are going to be enough. Nevertheless, if we think that in intuitionistic Logic or fragments of classical Arithmetic [7] general permutation rules are not needed to compute witnesses, it should not entirely come as a surprise that this is still the case in our framework.

■ **Proposition 16** (Normal Form Property). *Let* $\mathsf{P}, \mathsf{P}_1, \ldots, \mathsf{P}_n$ *be negative propositional formulas. Suppose that*

$$\Gamma = x_1 : \mathsf{P}_1, \ldots, x_n : \mathsf{P}_n, a_1 : \forall\alpha_1 A_1, \ldots, a_m : \forall\alpha_m A_m,$$

and $\Gamma \vdash t : \exists\alpha\,\mathsf{P}$ *or* $\Gamma \vdash t : \mathsf{P}$*, with* $t \in \mathsf{NF}$ *and having all its free variables among* $x_1, \ldots, x_n, a_1, \ldots, a_m$*. Then:*

1. *Either every occurrence in t of every term $\mathtt{H}_{a_i}^{\forall\alpha_i A_i}$ is of the active form $\mathtt{H}_{a_i}^{\forall\alpha_i A_i} m$, where m term of $\mathcal{L}$; or t has an active subterm of the form $\mathtt{H}_{a_i}^{\forall\alpha_i A_i} m$, for some non simply universal formula A_i and term m of $\mathcal{L}$.*

2. *Either $t = (m, u)$ or $t = \lambda x\, u$ or $t = \langle u, v\rangle$ or $t = u \,|\, v$ or $t = u \blacklozenge_a v$ or $t = \mathtt{H}^{\mathsf{P}}$ or $t = x_i\, t_1\, t_2 \ldots t_n$ or $t = \mathtt{H}_{a_i}^{\forall\alpha A_i} m\, t_2 \ldots t_n$.*

Proof. We prove 1. and 2. simultaneously and by induction on t. There are several cases, according to the shape of t:

- $t = (m, u)$, $\Gamma \vdash t : \exists\alpha\, \mathsf{P}$ and $\Gamma \vdash u : \mathsf{P}[m/\alpha]$. We immediately get 1. by induction hypothesis applied to u, while 2. is obviously verified.

- $t = \lambda x\, u$, $\Gamma \vdash t : \mathsf{P} = \mathsf{Q} \to \mathsf{R}$ and $\Gamma, x : \mathsf{Q} \vdash u : \mathsf{R}$. We immediately get 1. by induction hypothesis applied to u, while 2. is obviously verified.

- $t = \langle u, v\rangle$, $\Gamma \vdash t : \mathsf{P} = \mathsf{Q} \wedge \mathsf{R}$, $\Gamma \vdash u : \mathsf{Q}$ and $\Gamma \vdash v : \mathsf{R}$. We immediately get 1. by induction hypothesis applied to u, while 2. is obviously verified.

- $t = u \,|\, v$, $\Gamma, a : \mathsf{Q} \vdash u : \exists\alpha\, \mathsf{P}$ (resp. $u : \mathsf{P}$) and $\Gamma, a : \neg\mathsf{Q} \vdash v : \exists\alpha\, \mathsf{P}$ (resp. $v : \mathsf{P}$). We immediately get the thesis by induction hypothesis applied to u and v, while 2. is obviously verified.

- $t = u \blacklozenge_a v$, $\Gamma, a : \forall\beta\, A \vdash u : \exists\alpha\, \mathsf{P}$ (resp. $u : \mathsf{P}$) and $\Gamma, a : \exists\beta\, A^{\perp} \vdash v : \exists\alpha\, \mathsf{P}$ (resp. $u : \mathsf{P}$). We first observe that a must occur free in u: otherwise, $t = u \blacklozenge_a v \mapsto u$, which would yield a contradiction, for $t \in \mathsf{NF}$. Now, by induction hypothesis, 1. holds with respect to u. Moreover, it cannot be that every occurrence in u of every hypothesis variable a_i, a is active: otherwise, in particular, u would have an active subterm of the form $\mathtt{H}_a^{\forall\alpha A} m$, for some $m \in \mathcal{L}$, and thus $t = u \blacklozenge_a v \mapsto v[a := n] \blacklozenge_b (u[a := n] \blacklozenge_a v)$, with $n = (m, b)$: but $t \in \mathsf{NF}$. Therefore, u has an active subterm of the form $\mathtt{H}_{a_i}^{\forall\alpha_i A_i} m$, for some non simply universal formula A_i and $m \in \mathcal{L}$. We have thus established 1. for t, while 2. is obviously verified.

- $t = \mathtt{H}_{a_i}^{\forall\alpha A_i}$. This case is not possible, for $\Gamma \vdash t : \exists\alpha\, \mathsf{P}$ or $\Gamma \vdash t : \mathsf{P}$.

- $t = \mathtt{H}^{\mathsf{P}}$. In this case, 1. and 2. are trivially true.

- t is obtained by an elimination rule and we write it as $r\, t_1\, t_2 \ldots t_n$ (this notation has been explained in Section 2). Notice that in this case r cannot be a redex neither a term of the form $u \blacklozenge_a v$ nor $u \,|\, v$ because of the permutation rules and $t \in \mathsf{NF}$). We have now two cases:

  1. $r = x_i$ (resp. $r = \mathtt{H}^{\mathsf{P}}$). Then, since $\Gamma \vdash x_i : \mathsf{P}_i$ (resp. $\Gamma \vdash \mathtt{H}^{\mathsf{P}} : \mathsf{P}$), we have that for each i, either t_i is π_j or $\Gamma \vdash t_i : \mathsf{Q}$, where Q is a propositional formula. By induction hypothesis, each t_i satisfies 1. and thus also t. 2. is obviously verified.

  2. $r = \mathtt{H}_{a_i}^{\forall\alpha_i A_i}$. Then, t_1 is m, for some closed term of $\mathcal{L}$. If A_i is not simply universal, we obtain that t satisfies 1., for $t = \mathtt{H}_{a_i}^{\forall\alpha A_i} m\, t_2 \ldots t_n$. If $A_i = \forall\gamma_1 \ldots \gamma_k\, \mathsf{Q}$, with Q propositional, we have that for each i, either t_i is a closed term m_i of $\mathcal{L}$ or t_i is π_j or $\Gamma \vdash t_i : \mathsf{R}$, where R is a propositional formula. By induction hypothesis, each t_i satisfies 1. and thus also t. 2. is obviously verified.

◀

If we omit parentheses, every normal proof-term can be written as $v_0 \mid v_1 \mid \ldots \mid v_n$, where each v_i is not of the form $u \mid v$; if for every i, v_i is of the form (m_i, u_i), then we call the whole term a *Herbrand normal form*, because it is essentially a list of the witnesses appearing in a Herbrand disjunction. Formally:

■ **Definition 17** (Herbrand Normal Forms)**.** We define by induction a set of proof terms, called *Herbrand normal forms*, as follows:

- Every normal proof-term (t, u) is a Herbrand normal form;
- if u and v are Herbrand normal forms, $u \mid v$ is a Herbrand normal form.

Our last task is to prove that all quasi-closed proofs of a simply existential statement $\exists\alpha\,\mathsf{P}$ include an exhaustive sequence $m_1, m_2, \ldots, m_k$ of possible witnesses.

■ **Theorem 18** (Herbrand Disjunction Extraction)**.** *Let $\exists\alpha\,\mathsf{P}$ be any closed formula where P is negative. Suppose $\Gamma \vdash t : \exists\alpha\,\mathsf{P}$, t is quasi-closed and $t \mapsto^* t' \in \mathsf{NF}$. Then $\Gamma \vdash t' : \exists\alpha\,\mathsf{P}$ and t' is a Herbrand normal form*

$$(m_0, u_0) \mid (m_1, u_1) \mid \ldots \mid (m_k, u_k)$$

Moreover, $\Gamma \vdash \mathsf{P}[m_1/\alpha] \vee \cdots \vee \mathsf{P}[m_k/\alpha]$.

Proof. We proceed by induction on t'. By the Subject Reduction Theorem 4, $t' : \exists\alpha\,\mathsf{P}$. By Proposition 16, t' can only have three possible shapes:

1. $t' = u \mathbin{\rfloor}_a v$. We show that this cannot happen. First, a must occur free in u, otherwise $t' \notin \mathsf{NF}$. By Proposition 16, we have two possibilities. i) Every occurrence in u of every term $\mathtt{H}_{a_i}^{\forall\alpha_i A_i}$, with a_i free, is of the active form $\mathtt{H}_{a_i}^{\forall\alpha_i A_i} m$, where $m \in \mathcal{L}$; in particular this is true when $a_i = a$, which implies $t' \notin \mathsf{NF}$. ii) u has a active subterm of the form $\mathtt{H}_{a_i}^{\forall\alpha_i A_i} m$, for some non simply universal formula A_i and $m \in \mathcal{L}$: since t' is quasi-closed, $a_i = a$, which again implies $t' \notin \mathsf{NF}$. In any case, we have a contradiction.
2. $t' = u \mid v$; then, by induction hypothesis, u, v are Herbrand normal forms, and thus by definition 17, t' is an Herbrand normal form as well.
3. $t' = (m, u)$; then, we are done.

We have thus shown that t' is a Herbrand normal form

$$(m_0, u_0) \mid (m_1, u_1) \mid \ldots \mid (m_k, u_k)$$

Finally, we have that for each i, $\Gamma_i \vdash u_i : \mathsf{P}[m_i/\alpha]$, for the very same Γ_i that types (m_i, u_i) of type $\exists\alpha\,\mathsf{P}$ in t'. Therefore, for each i, $\Gamma_i \vdash u_i^+ : \mathsf{P}[m_1/\alpha] \vee \cdots \vee \mathsf{P}[m_k/\alpha]$, where u_i^+ is of the form $\iota_{i_1}(\ldots \iota_{i_k}(u_i)\ldots)$. We conclude that

$$\Gamma \vdash u_0^+ \mid u_1^+ \mid \ldots \mid u_k^+ : \mathsf{P}[m_1/\alpha] \vee \cdots \vee \mathsf{P}[m_k/\alpha]$$

◀

We suggest to interpret an Herbrand normal form $(m_0, u_0) \mid (m_1, u_1) \mid \ldots \mid (m_k, u_k)$ in the following way. Each (m_i, u_i) represents the result of an intuitionistic computation of a witness in a possible universe; each time in an intuitionistic computation an exception is raised, a pair of alternative universes is generated. For each particular computation of each of the parallel universes to go through, one need to replace symbols of the form $\mathtt{W}_a^{\exists\alpha A}$ with actual terms of $\mathcal{L}$ (those are the only symbols that can really block the computation). These witnesses have been obtained by communications coming from other intuitionistic computations in other parallel universes. It is that process of interaction and dialogue between different possible computations that generate the Herbrand normal forms.

References

1 Akama, Y. and Berardi, S. and Hayashi S. and Kohlenbach, U.. *An Arithmetical Hierarchy of the Law of Excluded Middle and Related Principles*. LICS 2004, pages 192-201.

2 F. Aschieri, S. Berardi, *Interactive Learning-Based Realizability for Heyting Arithmetic with EM1*, Logical Methods in Computer Science, 2010.

3 F. Aschieri, S. Berardi, *A New Use of Friedman's Translation: Interactive Realizability*, in: Logic, Construction, Computation, Berger et al. eds, Ontos-Verlag Series in Mathematical Logic, 2012.

4 F. Aschieri, *Interactive Realizability for Classical Peano Arithmetic with Skolem Axioms*. Proceedings of Computer Science Logic 2012, Leibniz International Proceedings in Informatics, vol. 16, 2012.

5 F. Aschieri, *Interactive Realizability for Second-Order Heyting Arithmetic with $EM1$ and $SK1$*, Mathematical Structures in Computer Science, 2013.

6 F. Aschieri, *Strong Normalization for HA + EM1 by Non-Determinstic Choice*, Proceeding of First Workshop on Control Operators and their Semantics 2013 (COS 2013), Electronic Proceedings in Theoretical Computer Science, vol. 127, 2013

7 F. Aschieri, S. Berardi, G. Birolo, *Realizability and Strong Normalization for a Curry-Howard Interpretation of HA + EM1*, Proceedings of Computer Science Logic 2013, Leibniz International Proceeding in Computer Science, vol. 23, 2013.

8 F. Aschieri, M. Zorzi: *Non-Determinism, Non-Termination and the Strong Normalization of System T*, Proceedings of TLCA 2013, vol. 7941, 31–47, 2013.

9 S. Berardi and U. de' Liguoro, *Interactive Realizers. A New Approach to Program Extraction from Nonconstructive Proofs*, Transaction of Computational Logic, vol. 13, n. 2, 2012.

10 G. Birolo: *Interactive Realizability, Monads and Witness Extraction*, Ph.D. thesis, April, 15, 2013, Università di Torino (http://arxiv.org/abs/1304.4091)

11 S. Buss, *On Herbrand's Theorem*, in Logic and Computational Complexity, LNCS, n. 960, Springer-Verlag, 1995.

12 T. Coquand, *A Semantic of Evidence for Classical Arithmetic*, Journal of Symbolic Logic, vol. 60, pp. 325-337,1995.

13 U. Dal Lago, M. Zorzi, *Probabilistic Operational Semantics for the Lambda Calculus*. RAIRO - Theoretical Informatics and Applications, DOI 10.1051/ita/2012012, vol. 46 , n. 03 , 2012 , pp. 413-450, CUP, (2012)

14 de' Liguoro, U., Piperno, A.: *Non-Deterministic Extensions of Untyped Lambda-Calculus*. Information and Computation **122** (1995) 149–177.

15 J.-Y. Girard and Y. Lafont and P. Taylor.: *Proofs and Types*. Cambridge University Press (1989).

16 G. Gentzen, *Die Widerspruchsfreiheit der reinen Zahlentheorie*. Mathematische Annalen, 1935.

17 P. de Groote, *A Simple Calculus of Exception Handling*, Proc. of TLCA 1995: 201–215.

18 P. de Groote, *Strong Normalization for Classical Natural Deduction with Disjunction*, Proceedings of TLCA 2001: 182–196.

19 H. Herbelin, *An Intuitionistic Logic that Proves Markov's Principle*, Proceedings of LICS 2010: 50-56.

20 G. Kreisel, *On the Interpretation on Non-Finitist Proofs: Part II*, The Journal of Symbolic Logic, vol. 17, n.1, 43–58, 1952.

21 G. Kreisel, *On Weak Completeness of Intuitionistic Predicate Logic*, Journal of Symbolic Logic, vol. 27, 1962.

22 G. Mints, *A Method of Epsilon Substitution for Predicate Logic with Equality*, Journal of Mathematical Sciences, vol. 87, n. 1, 1997.

23 G. Mints, S. Tupailo, W. Bucholz, *Epsilon Substitution Method for Elementary Analysis*, Archive for Mathematical Logic, volume 35, 1996

24 D. Prawitz: *Ideas and Results in Proof Theory*. In Proceedings of the Second Scandinavian Logic Symposiuum (1971).

25 M. H. Sorensen, P. Urzyczyn, *Lectures on the Curry-Howard isomorphism*, Studies in Logic and the Foundations of Mathematics, vol. 149, Elsevier, 2006.

26 J. von Plato: *Genzen's Proof of Normalization for Natural Deduction*, Bulletin of Symbolic Logic, vol. 14, n. 2, 2008.