Realizability and Strong Normalization for a Curry-Howard Interpretation of HA + EM1

Federico Aschieri*[1], Stefano Berardi[2], and Giovanni Birolo[3]

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 Torino, Italy**
3 **Dipartimento di Matematica, Università di Torino, Italy**

Abstract

We present a new Curry-Howard correspondence for $\mathsf{HA}+\mathsf{EM}_1$, constructive Heyting Arithmetic with the excluded middle on Σ^0_1-formulas. We add to the lambda calculus an operator $\|_a$ which represents, from the viewpoint of programming, an exception operator with a delimited scope, and from the viewpoint of logic, a restricted version of the excluded middle. We motivate the restriction of the excluded middle by its use in proof mining; we introduce new techniques to prove strong normalization for $\mathsf{HA}+\mathsf{EM}_1$ and the witness property for simply existential statements. One may consider our results as an application of the ideas of Interactive realizability, which we have adapted to the new setting and used to prove our main theorems.

1998 ACM Subject Classification F.4.1

Keywords and phrases Interactive realizability, classical Arithmetic, witness extraction, delimited exceptions

Digital Object Identifier 10.4230/LIPIcs.xxx.yyy.p

1 Introduction

From the beginning of proof theory many results have been obtained which clearly show that classical proofs have a constructive content. The seminal results are Hilbert's epsilon substitution method (see e.g [23]) and Gentzen's cut elimination [12]. Then, several other techniques have been introduced: among them, Gödel's double negation translation followed either by the Gödel functional interpretation [11] or Kreisel's modified realizability [18] and Friedman's translation [10]; the Curry-Howard correspondence between natural deduction and programming languages (see e.g. [27]).

In this paper we follow the Curry-Howard line of research. But what does it mean to extract constructive content from a natural deduction proof? Essentially, it means interpreting the positive connectives $\vee, \exists$ *as positively as possible*, that is, recovering information about truth as much as possible. The problem is that, even in intuitionistic Arithmetic, a disjunction $A \vee B$ can be proven without explicitly proving A or proving B; a proof of an existential statement $\exists \alpha^{\mathtt{N}} A$ may be accepted even if it does not directly provide a witness, i.e. a number n and a proof that $A[n/\alpha]$ holds. It is the very shape of the natural deduction rules that allows that: there are not only inference rules for direct arguments – *introduction* rules – but also indirect elimination rules. One can then prove a disjunction by an elimination rule, for

* 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)

example as a consequence of a general inductive argument for a formula $\forall \alpha^{\mathtt{N}}. A(\alpha) \vee B(\alpha)$ and then conclude $A(0) \vee B(0)$. It is a remarkable result of proof theory that it is possible to give a complete simple classification of the *detours* that can occur in an *intuitionistic* arithmetical proof, which are small pieces of indirect reasoning that can be readily eliminated through a simple proof transformation. Once this detours are eliminated, one obtains direct proofs of disjunctions or existential statements (see Prawitz [26]).

For classical Arithmetic, the situation may appear desperate: the double negation elimination rule $\neg\neg A \to A$ is a so indirect way of arguing, that seems impossible to be eliminated; the excluded middle $A \vee \neg A$ allows a disjunction to be asserted without having the slightest idea of which side holds. Indeed, for a long time, there has not been a set of reduction rules, nor a notion of classical detour, that worked for proofs containing *all* the logical connectives. It was Griffin [15] who gave a very elegant reduction rule for eliminating the double negation elimination. If A is concluded from $\neg\neg A$ and then used to prove $\perp$, then one can capture the part of the proof that surrounds A to obtain a proof of $\neg A$ and give it to the premiss $\neg\neg A$ in order to get a more direct proof of $\perp$. While this idea was initially applied only to negative fragments of Arithmetic, it became clear that it could be adapted even to a full set of connectives.

It was in that way that control operators entered the scene. The proof reductions for classical Arithmetic can be implemented by a Curry-Howard correspondence between proofs and functional languages enriched with operators that can capture the computational context. Several languages have been put forward for that aim. Griffin proposed the lambda calculus plus $\mathsf{call/cc}$, solution that has been developed and extended by Krivine [21, 22] with remarkable success. Parigot [25] put forward the $\lambda\mu$-calculus, which enjoys many of the nice properties of the lambda calculus that are instead lost when using $\mathsf{call/cc}$; de Groote [14] extended the $\lambda\mu$-calculus in order to interpret primitively all the logical connectives.

After these works, it became evident that enriching functional languages with other "less pure" computational constructs would allow to implement reduction rules for many mathematical axioms. For example, Krivine used the instruction quote to provide computational content to the axiom of dependent choice. Recently, Herbelin [16] has used the mechanism of delimited exceptions to give special reduction rules for Markov's principle.

The goal of this paper is to use a new combination of known computational constructs in order to interpret Heyting Arithmetic HA with the excluded middle schema EM_1, $\forall \alpha^{\mathtt{N}} \mathsf{P} \vee \exists \alpha^{\mathtt{N}} \mathsf{P}^{\perp}$, where P is any atomic decidable predicate (see [1]) and $\mathsf{P}^{\perp}$ denotes the atomic decidable predicate which is its complement. We shall give new reduction rules for $\mathsf{HA} + \mathsf{EM}_1$, and introduce a realizability semantics in order to investigate, describe and prove properties of their behavior. We shall use delimited exceptions, and permutative conversions for disjunction elimination. Permutative rules were introduced by Prawitz (see [26]) to obtain the subformula property in first-order natural deductions: in our framework, they will naturally express control operators. Delimited exceptions were used by de Groote [13] in order to interpret the excluded middle in classical propositional logic with implication; by Herbelin [16], in order to pass witnesses to some existential formula when a falsification of its negation is encountered. We shall use exceptions in a similar way, and our work may be seen as a modification and extension of some of de Groote's and Herbelin's techniques. Our reduction rules for the classical principle EM_1 are inspired by Interactive realizability [2, 3] for $\mathsf{HA} + \mathsf{EM}_1$, which describes classical programs as programs that *make hypotheses*, *test them* and *learn by refuting* the incorrect ones. The interest of EM_1 lies in the fact that this classical principle is logically simple, yet it may formalize many classical proofs: for instance, proofs of Euclidean geometry (like Sylvester conjecture, see J. von Plato [28]), of Algebra (like Dickson's Lemma, see S. Berardi [7]) and of Analysis (those using Koenig's Lemma, see Kohlenbach [17]).

We now give an high level explanation of our contributions and of how they compare to other interpretations of classical proofs.

1.1 Excluded Middle versus Double Negation Elimination

As we have said, control operators have been mainly used to interpret primitively double negation elimination, or some related principle (as the Pierce law: $(\neg A \to A) \to A$). To interpret the excluded middle with this approach, one first proves intuitionistically $\bot$ (and thus EM) from $\neg\mathsf{EM}$ and then applies the rules of double negation elimination or Pierce law to obtain a proof term for EM. In this way, however, one does not address directly the excluded middle and sticks to an implicit negative translation which eliminates it. But what is classical logic if not the conception that formulas speak about models, and a formula is either true or false? It is also evident that the real idea behind the constructivization of classical logic is concealed in the proof of $\neg\neg\mathsf{EM}$: it is there that it is really determined *what is the use* of the continuations produced by control operators and *why* it is needed.

In this paper, we give direct reduction rules for the excluded middle EM_1. We treat it as an elimination rule, as in [13] and in the actual mathematical practice:

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

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

1.2 Permutation Rules for EM_1

We solve the problem as in [13] by adding permutation rules, as usual with disjunction. For example, $(u \parallel_a v)w$ reduces to $uw \parallel_a vw$. In this way, one obtains two important results: first, one may explore *both* the possibilities, $\forall\alpha^{\mathtt{N}}\mathsf{P}$ is true or $\exists\alpha^{\mathtt{N}}\mathsf{P}^{\perp}$ is true, and evaluate uw and vw; second, one duplicates the applicative context $[\,]w$, which will be needed in case of backtracking from the branch uw to vw. If $C = A \wedge B$, one may form the proof term $\pi_0(u \parallel_a v)$, which reduces to $\pi_0 u \parallel_a \pi_0 v$, 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, $\parallel$ behaves like a control-like operator.

1.3 Delimited Exceptions

The reductions that we put forward for the new proof terms $u \parallel_a v$ are inspired by the informal idea of learning by making falsifiable hypotheses. When normalizing a term $u \parallel_a v$, we shall consider u as the *active branch*. The reason is that the hypothesis $\forall\alpha^{\mathtt{N}}\mathsf{P}$ has no computational content, and it is only a certificate *serving to guarantee the correctness* of

u. Therefore, one can "run" u making the hypothesis $\forall\alpha^{\mathtt{N}}\mathsf{P}$ without the risk that the computation will be blocked; on the contrary, the branch v cannot a priori be executed without that risk, because the hypothesis $\exists\alpha^{\mathtt{N}}\mathsf{P}^{\perp}$ has a computational content (a witness) that may be requested in order to go on with the computation. That does not mean that one is not free to first perform reductions inside v, but rather that one may not expect to necessarily get useful results in that branch.

The informal idea expressed by our reductions is thus to assume $\forall\alpha^{\mathtt{N}}\mathsf{P}$ and try to produce some proof of C out of u by reducing inside u. The crucial intuition – recurring again and again in proof theory – is that when C is a concrete statement, for example a simple existential formula, one actually needs only a finite number of instances of $\forall\alpha^{\mathtt{N}}\mathsf{P}$ to prove it. Whenever u needs the truth of an instance $\mathsf{P}[n/\alpha]$ of the assumption $\forall\alpha^{\mathtt{N}}\mathsf{P}$, 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 $\forall\alpha^{\mathtt{N}}\mathsf{P}$ being checked are true, *and no assumption* $\forall\alpha^{\mathtt{N}}\mathsf{P}$ *is left* (this is the non-trivial part), then the normal form u' of u is *independent* from $\forall\alpha^{\mathtt{N}}\mathsf{P}$ and we found some $u' : C$. Remark that, in this case, we do not know whether $\forall\alpha^{\mathtt{N}}\mathsf{P}$ is true or false, because u only checked finitely many instances of it: all we do know is that the full hypothesis $\forall\alpha^{\mathtt{N}}\mathsf{P}$ is unnecessary in proving C. If instead some assumption of $\forall\alpha^{\mathtt{N}}\mathsf{P}$ is left in u we are stuck. There is only one way out of this impasse and can occur at any moment: u may find some instance $\mathsf{P}[n/\alpha]$ which is false, and thus refute the assumption $\forall\alpha^{\mathtt{N}}\mathsf{P}$. In this case the attempt of proving C from $\forall\alpha^{\mathtt{N}}\mathsf{P}$ fails, we obtain $\mathsf{P}^{\perp}[n/\alpha]$ and u *raises the exception* n; from the knowledge that $\mathsf{P}^{\perp}[n/\alpha]$ holds, a canonical proof term $\exists\alpha^{\mathtt{N}}\mathsf{P}^{\perp}$ is formed and passed to v: a proof term for C has now been obtained and it can be executed.

In order to implement those reductions we shall use constant terms of the form $\mathtt{H}^{\forall\alpha\mathsf{P}}$, whose task is to take a numeral n and reduce to $\mathtt{True}$ if $\mathsf{P}[n/\alpha]$ holds, otherwise raise an exception. We shall also use a constant $\mathtt{W}^{\exists\alpha\mathsf{P}^{\perp}}$ denoting some unknown proof term for $\exists\alpha^{\mathtt{N}}\mathsf{P}^{\perp}$, whose task is to *catch* the exception raised by $\mathtt{H}^{\forall\alpha\mathsf{P}}$. Actually, these terms will occur only through typing rules of the form

$$\Gamma, a : \forall\alpha^{\mathtt{N}}\mathsf{P} \vdash [a]\mathtt{H}^{\forall\alpha\mathsf{P}} : \forall\alpha^{\mathtt{N}}\mathsf{P} \qquad \Gamma, a : \exists\alpha^{\mathtt{N}}\mathsf{P}^{\perp} \vdash [a]\mathtt{W}^{\exists\alpha\mathsf{P}^{\perp}} : \exists\alpha^{\mathtt{N}}\mathsf{P}^{\perp}$$

where a is used just as a name of a communication channel for exceptions: if in u occurs a subterm of the form $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}n$, where the closed expression $\mathsf{P}[n/\alpha]$ is false, then $u \parallel_a v$ reduces to $v[a := n]$, which denotes the result of the replacement of $[a]\mathtt{W}^{\exists\alpha\mathsf{P}^{\perp}}$ in v with the proof term $(n, \mathtt{True})$. From the viewpoint of programming, that is a *delimited exception* mechanism (see de Groote [13] and Herbelin [16] 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. As pointed out to us by H. Herbelin, the whole term $u \parallel_a v$ can also be expressed in a standard way by the constructs raise and $\mathsf{try} \ldots \mathsf{with} \ldots$ in the CAML programming language.

1.4 Realizability and Prawitz Validity

We now have a set of detour conversions for $\mathsf{HA} + \mathsf{EM}_1$: which notion of construction does it determine? The normalization process, even in intuitionistic logic, tends to be obscure: while the local meaning of reduction steps is clear, the global behaviour of the procedure is harder to grasp. This is the reason why it is important to define proof-theoretic semantics, in particular those who have the task of explaining what is a construction in intuitionistic or classical sense. Realizability is one of those semantics. In analogy with the discussion in Prawitz [26] about validity, one may classify realizabilities in two groups: those who give priority to introduction rules and those who rather privilege elimination rules in order to give meaning to logical connectives.

Realizabilities based on introduction rules. In this case, one explains a logical constant in term of the construction given by an introduction rule for that constant. For example, a realizer of $A \wedge B$ is a pair made by a realizer of A and a realizer B; a realizer of $A \vee B$ contains either a realizer of A or a realizer of B together with an indication of which formula is realized. Of course, this approach tends to work with constructive logics, which have the disjunction and numerical existence properties. Prawitz's notion of validity and Kreisel modified realizability are witness to that. There is one exception: Interactive realizability [3, 4], which explains positive classical connectives with introduction rules thanks to the use of the concept of state of knowledge.

Realizability based on elimination rules. In this case, one describes the meaning of a logical constant in terms of "performability of operations" or in terms of what can be obtained by the elimination rules for that constant. This approach works very well for negative connectives, and in fact is not very different from the one given by introduction rules: but since it has a semantical flavor, it is usually the preferred one. At the time of Prawitz [26], it seemed impossible that this approach could work also for positive connectives, given the circularity involved in the elimination rules (in terms of logical complexity). It was only after Girard's reducibility [9], and the work of Krivine [19, 21], that the second order definition of $A \vee B$ as $\forall X. (A \to X) \to (B \to X) \to X$ has been exploited for defining a realizability based on elimination rules. While remarkable, this result makes classical realizabilities based on elimination rules equivalent to some negative translation, re-proposing at the semantical level the issue which is eliminated on the syntactical one. Indeed, all realizabilities proposed for languages based on control operators are equivalent to some negative translation [24] (not surprisingly, since these operators were originally devised to interpret directly double negation elimination).

In this paper, we shall present a classical realizability borrowing ideas from both groups. The treatment of negative logical constants will be à la Kreisel, while the positive ones will be treated à la Prawitz. In particular the set of realizers of $A \vee B$ and of $\exists \alpha^{\mathtt{N}} A$ will be constructed by an inductive definition whose base case is an introduction rule; the atomic realizers will represent proofs in "extended" Post systems. This gives, first, an adaptation of Interactive realizability to a language with exceptions and control operators; second, an extension of Prawitz's notion of validity to a system with classical principles. We find these achievements interesting in their own right, because of the semantical meaning of validity given by Prawitz [26]. It seems also that our approach is not equivalent in any straightforward sense to a negative translation, in line with our desire of interpreting positive connectives *as positively as possible.*

1.5 Witness Extraction and Strong Normalization

Thanks to realizability, we shall provide a new semantical proof of a *normal form result* syntactically proven by Birolo [8], expressing that any closed normal proof term whose type is a simply existential formula $\exists \alpha^{\mathtt{N}} \mathsf{P}$ provides a witness through the process sketched above (that is, one never gets stuck with simply existential formulas); and a new *strong normalization result*, proving that all reduction paths terminate into a normal form. We anticipate that in our calculus all the reduction strategies are allowed, therefore strong normalization is not the same thing as weak normalization, as for example in Krivine's realizability [19]. This freedom is desirable, because it avoids artificial programming constraints which complicate the writing of realizers.

We remark that we cannot prove the witness property for all existential statements of $\mathsf{HA} + \mathsf{EM}_1$. Indeed, using EM_1 we may prove paradoxical statements like the drinker principle

$\exists\alpha^{\mathtt{N}}\forall\beta^{\mathtt{N}}.\,\mathsf{P}(\alpha)\to\mathsf{P}(\beta)$, for P primitive recursive, but for some P there is no map computable in the parameters of P providing some n such that $\forall\beta^{\mathtt{N}}.\,\mathsf{P}(n)\to\mathsf{P}(\beta)$. However we prove the witness property for all Π^0_2-statements of $\mathsf{HA}+\mathsf{EM}_1$, which include all statements about convergence of algorithms, therefore all statements more interesting for Computer Science. The witness property we prove is a particular case of the witness property which holds for the entire classical arithmetic by the results of Gödel: the interest of our results lies in the new reduction set we provide and in their semantics.

1.6 Non-Determinism

We anticipate that our set of reductions is non-deterministic, i.e. non-confluent. Whenever there are two false instances $\mathsf{P}[n/\alpha]$, $\mathsf{P}[m/\alpha]$ of an hypothesis $\forall\alpha^{\mathtt{N}}\mathsf{P}$ in some EM_1-rule $u\parallel_a v$, in u it may be raised either the exception n related to $\mathsf{P}[n/\alpha]$, or the exception m related to $\mathsf{P}[m/\alpha]$. The computation is converging in both cases, and the witness we get for a simple existential conclusion C is correct in both cases: however, we may obtain a *different* witness in the two cases. The interest of the non-deterministic approach is that it does not impose arbitrary restrictions ruling out potentially interesting computations: there are classical proofs whose non-deterministic interpretation is in a sense canonical (see [6], p. 40-50 for examples). Alternatively, with techniques introduced in [2], we may provide in a simple and natural way confluent evaluation rules. It is an interesting aspect of our framework that non-determinism arises just because one may generate during computation different refutations of EM_1-hypotheses, so any strategy for choosing between them re-establishes confluence. For reason of space, we shall not address this matter in the present paper.

1.7 Plan of the Paper

This is the plan of the paper. In §2 we introduce a type theoretical version of intuitionistic arithmetic HA extended with EM_1. In §3 we introduce a realizability semantics for $\mathsf{HA}+\mathsf{EM}_1$. Then in §4, 5 we prove that this semantics is sound for $\mathsf{HA}+\mathsf{EM}_1$. As a corollary, we deduce that $\mathsf{HA}+\mathsf{EM}_1$ is strongly normalizing and that any proof of a simply existential Σ^0_1-formula provides a witness.

2 The System $\mathsf{HA}+\mathsf{EM}_1$

In this section we formalize intuitionistic Arithmetic HA, and we add an operator $\parallel$ formalizing EM_1. We start with the language of formulas.

▶ **Definition 1** (Language of $\mathsf{HA}+\mathsf{EM}_1$)**.** The language $\mathcal{L}$ of $\mathsf{HA}+\mathsf{EM}_1$ is defined as follows.

1. The terms of $\mathcal{L}$ are inductively defined as either variables $\alpha,\beta,\ldots$ or 0 or $\mathsf{S}(t)$ with $t\in\mathcal{L}$. A numeral is a term of the form $\mathsf{S}\ldots\mathsf{S}0$.

2. There is one symbol $\mathcal{P}$ for every primitive recursive relation over $\mathbb{N}$; with $\mathcal{P}^{\perp}$ we denote the symbol for the complement of the relation denoted by $\mathcal{P}$. The atomic formulas of $\mathcal{L}$ are all the expressions of the form $\mathcal{P}(t_1,\ldots,t_n)$ such that $t_1,\ldots,t_n$ are terms of $\mathcal{L}$ and n is the arity of $\mathcal{P}$. Atomic formulas will also be denoted as $\mathsf{P},\mathsf{Q},\mathsf{P}_i,\ldots$.

3. The formulas of $\mathcal{L}$ are built from atomic formulas of $\mathcal{L}$ by the connectives $\vee,\wedge,\to,\forall,\exists$ as usual, with quantifiers ranging over numeric variables $\alpha^{\mathtt{N}},\beta^{\mathtt{N}},\ldots$.

From now on, if P is any *closed* atomic formula, we will write $\mathsf{P} \equiv \mathtt{True}$ ($\mathsf{P} \equiv \mathtt{False}$) if the formula is true (false) in the standard interpretation, that is, if $\mathsf{P} = \mathcal{R}(n_1, \ldots, n_k)$ and the sequence of numerals $(n_1, \ldots, n_k)$ belongs (does not belong) to the primitive recursive relation denoted by $\mathcal{R}$. We now define in figure 1 a set of untyped proof terms, then a type assignment for them. It is a standard natural deduction system with introduction and

Grammar of Untyped Proof Terms

$$t, u, v ::= \ x \mid tu \mid tm \mid \lambda xu \mid \lambda \alpha u \mid \langle t, u\rangle \mid \pi_0 u \mid \pi_1 u \mid \iota_0(u) \mid \iota_1(u) \mid t[x.u, y.v] \mid (m, t) \mid t[(\alpha, x).u]$$

$$\mid u \parallel_a v \mid [a]\mathtt{H}^{\forall \alpha \mathsf{P}} \mid [a]\mathtt{W}^{\exists \alpha \mathsf{P}^\perp} \mid \mathtt{True} \mid \mathsf{R}uvm \mid \mathsf{r}t_1 \ldots t_n$$

where m ranges over terms of $\mathcal{L}$, x over proof terms variables and a over hypothesis variables. We also assume that in the term $u \parallel_a v$, there is some atomic formula P, such that a occurs free in u only in subterms of the form $[a]\mathtt{H}^{\forall \alpha \mathsf{P}}$ and a occurs free in v only in subterms of the form $[a]\mathtt{W}^{\exists \alpha \mathsf{P}^\perp}$, and the occurrences of the variables in P 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_1 hypothesis variable $a, b, \ldots$, and $e_i \neq e_j$ for $i \neq j$.

Axioms $\Gamma, x : A \vdash x : A \qquad \Gamma, a : \forall \alpha^{\mathtt{N}} \mathsf{P} \vdash [a]\mathtt{H}^{\forall \alpha \mathsf{P}} : \forall \alpha^{\mathtt{N}} \mathsf{P} \qquad \Gamma, a : \exists \alpha^{\mathtt{N}} \mathsf{P}^\perp \vdash [a]\mathtt{W}^{\exists \alpha \mathsf{P}^\perp} : \exists \alpha^{\mathtt{N}} \mathsf{P}^\perp$

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

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

Disjunction Intro. $\dfrac{\Gamma \vdash u : A}{\Gamma \vdash \iota_0(u) : A \vee B} \qquad \dfrac{\Gamma \vdash u : B}{\Gamma \vdash \iota_1(u) : A \vee B}$

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 $\dfrac{\Gamma \vdash u : \forall \alpha^{\mathtt{N}} A}{\Gamma \vdash um : A[m/\alpha]} \quad \dfrac{\Gamma \vdash u : A}{\Gamma \vdash \lambda \alpha u : \forall \alpha^{\mathtt{N}} A}$

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

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

Induction $\dfrac{\Gamma \vdash u : A(0) \quad \Gamma \vdash v : \forall \alpha^{\mathtt{N}}. A(\alpha) \to A(\mathsf{S}(\alpha))}{\Gamma \vdash \mathsf{R}uvt : A(t)}$

where t is any term of the language $\mathcal{L}$.

Post Rules $\dfrac{\Gamma \vdash u_1 : \mathsf{P}_1 \ \Gamma \vdash u_2 : \mathsf{P}_2 \ \cdots \ \Gamma \vdash u_n : \mathsf{P}_n}{\Gamma \vdash u : \mathsf{P}}$

where $\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_n, \mathsf{P}$ are atomic formulas and the rule is a Post rule for equality, for a Peano axiom or a primitive recursive relation and if $n > 0$, u is $\mathsf{r}u_1 \ldots u_n$, otherwise u is $\mathtt{True}$.

EM1 $\dfrac{\Gamma, a : \forall \alpha^{\mathtt{N}} \mathsf{P} \vdash w_1 : C \quad \Gamma, a : \exists \alpha^{\mathtt{N}} \mathsf{P}^\perp \vdash w_2 : C}{\Gamma \vdash w_1 \parallel_a w_2 : C}$

Figure 1 Term Assignment Rules for $\mathsf{HA} + \mathsf{EM}_1$

elimination rules for each connective and induction rules for integers, together with a term assignment in the spirit of Curry-Howard correspondence (see [27], for example).

We replace purely universal axioms (i.e., Π^0_1-axioms) with Post rules (as in Prawitz [26]), which are inferences of the form

$$\frac{\Gamma \vdash \mathsf{P}_1 \quad \Gamma \vdash \mathsf{P}_2 \ \cdots \quad \Gamma \vdash \mathsf{P}_n}{\Gamma \vdash \mathsf{P}}$$

where $\mathsf{P}_1, \ldots, \mathsf{P}_n, \mathsf{P}$ are atomic formulas of $\mathcal{L}$ such that for every substitution $\sigma = [t_1/\alpha_1, \ldots, t_k/\alpha_k]$ of closed terms $t_1, \ldots, t_k$ of $\mathcal{L}$, $\mathsf{P}_1\sigma = \ldots = \mathsf{P}_n\sigma \equiv \mathtt{True}$ implies $\mathsf{P}\sigma \equiv \mathtt{True}$. Let now eq be the symbol for the binary relation of equality between natural numbers ("$=$" will also be used). Among the Post rules, we have the Peano axioms

$$\frac{\Gamma \vdash \mathsf{eq}(\mathsf{S}t_1, \mathsf{S}t_2)}{\Gamma \vdash \mathsf{eq}(t_1, t_2)} \qquad \frac{\Gamma \vdash \mathsf{eq}(0, \mathsf{S}t)}{\Gamma \vdash \bot}$$

and axioms of equality

$$\frac{}{\Gamma \vdash \mathsf{eq}(t, t)} \qquad \frac{\Gamma \vdash \mathsf{eq}(t_1, t_2) \quad \Gamma \vdash \mathsf{eq}(t_2, t_3)}{\Gamma \vdash \mathsf{eq}(t_1, t_3)} \qquad \frac{\Gamma \vdash \mathsf{P}[t_1/\alpha] \quad \Gamma \vdash \mathsf{eq}(t_1, t_2)}{\Gamma \vdash \mathsf{P}[t_2/\alpha]}$$

We also have a Post rule for the defining axioms of each primitive recursive relation, for example the false relation $\bot$, addition, multiplication:

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \mathsf{P}} \qquad \frac{}{\Gamma \vdash \mathsf{add}(t, 0, t)} \qquad \frac{\Gamma \vdash \mathsf{add}(t_1, t_2, t_3)}{\Gamma \vdash \mathsf{add}(t_1, \mathsf{S}t_2, \mathsf{S}t_3)}$$

$$\frac{}{\Gamma \vdash \mathsf{mult}(t, 0, 0)} \qquad \frac{\Gamma \vdash \mathsf{mult}(t_1, t_2, t_3) \quad \Gamma \vdash \mathsf{add}(t_3, t_1, t_4)}{\Gamma \vdash \mathsf{mult}(t_1, \mathsf{S}t_2, t_4)}$$

For simplifying the representation of proofs, we assume also to have a Post rule for each true closed atomic formula P:

$$\frac{}{\Gamma \vdash \mathsf{P}}$$

From the $\bot$-rule for atomic formulas we may derive the $\bot$-rule for all formulas. We assume that in the proof terms three distinct classes of variables appear: one for proof terms, denoted usually as $x, y, \ldots$; one for quantified variables of the formula language $\mathcal{L}$ of $\mathsf{HA} + \mathsf{EM}_1$, denoted usually as $\alpha, \beta, \ldots$; one for the pair of hypotheses bound by EM_1, denoted usually as $a, b, \ldots$. In the term $u \parallel_a v$, any free occurrence of a in u occurs in an expression $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}$, and denotes an assumption $\forall\alpha^{\mathtt{N}}\mathsf{P}$. Any free occurrence of a in v occurs in an expression $[a]\mathtt{W}^{\exists\alpha\mathsf{P}^\perp}$, and denotes an assumption $\exists\alpha^{\mathtt{N}}\mathsf{P}^\perp$. All the occurrences of a in u and v are bound, and we assume the usual renaming rules and alpha equivalences to avoid capture of variables in the reduction rules that we shall give. Alternatively, $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}$ is the thrower of an exception a and $[a]\mathtt{W}^{\exists\alpha\mathsf{P}^\perp}$ is the catcher of the same exception a. With $u \parallel v$ we denote a generic term of the form $u \parallel_a v$; we shall use this notation whenever our considerations will not depend on which is exactly the variable a. Terms of the form $((u \parallel v_1) \parallel v_2)\ldots) \parallel v_n$ for any $n \geq 0$ will be denoted as $u \parallel v_1 \parallel \ldots \parallel v_n$ or as $\mathcal{EM}[u]$. In the terms $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}$ and $[a]\mathtt{W}^{\exists\alpha\mathsf{P}^\perp}$ the free variables are a and those of P minus α.

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. SN is the set of strongly normalizing untyped proof terms and NF is the set of normal untyped proof terms, as usual in lambda calculus ([27]). PNF is the inductively defined set of the Post normal forms (intuitively, normal terms representing closed proof trees made only of Post rules whose leaves are universal hypothesis followed by an elimination rule), that is: $\mathtt{True} \in \mathsf{PNF}$; for every closed term n of $\mathcal{L}$, if $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}n \in \mathsf{NF}$, then $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}n \in \mathsf{PNF}$; if $t_1, \ldots, t_n \in \mathsf{PNF}$, then $\mathsf{r}t_1 \ldots t_n \in \mathsf{PNF}$.

We are now going to explain the reduction rules for the proof terms of $\mathsf{HA}+\mathsf{EM}_1$, which are given in figure 2 (with $\mapsto^*$ we shall denote the reflexive and transitive closure of the one-step reduction $\mapsto$). We find among them the ordinary reductions of Intuitionistic Arithmetic for the logical connectives and induction. Permutation Rules for EM_1 are an instance of Prawitz's permutation rules for $\vee$-elimination, as explained in the introduction. Raising an exception n in $u \parallel_a v$ removes all occurrences of assumptions $[a]\mathtt{W}^{\exists\alpha\mathsf{P}^\perp}$ in v; we define first an operation removing them, and denoted $v[a := n]$.

▶ **Definition 2** (Witness Substitution)**.** Suppose v is any term and n a closed term of $\mathcal{L}$. We define

$$v[a := n]$$

as the term obtained from v by replacing each subterm $[a]\mathtt{W}^{\exists\alpha\mathsf{P}^\perp}$ corresponding to a free occurrence of a in v by $(n, \mathtt{True})$, if $\mathsf{P}[n/\alpha] \equiv \mathtt{False}$, and by $(n, [a]\mathtt{H}^{\forall\alpha\, \alpha=\mathsf{0}}\mathsf{S}0)$, otherwise.

▶ Remark. An exception is raised only when $\mathsf{P}[n/\alpha] \equiv \mathtt{False}$. Therefore the substitution of $[a]\mathtt{W}^{\exists\alpha\mathsf{P}^\perp}$ by $(n, [a]\mathtt{H}^{\forall\alpha\, \alpha=\mathsf{0}}\mathsf{S}0)$ will never occur in the reductions rules that we have defined. However, the general case of the substitution will be needed to define realizability, and namely because we want it to be suitable to prove strong normalization.

The rules for EM_1 translate the informal idea of learning by trial and error we sketched in the introduction, that is:

1. The first EM_1-reduction: $([a]\mathtt{H}^{\forall\alpha\mathsf{P}})n \mapsto \mathtt{True}$ if $\mathsf{P}[n/\alpha] \equiv \mathtt{True}$, says that whenever we use a closed instance $\mathsf{P}[n/\alpha]$ of the assumption $\forall\alpha^{\mathtt{N}}\mathsf{P}$, we check it, and if the instance is true we replace it with its canonical proof.
2. The second EM_1-reduction: $u \parallel_a v \mapsto u$, says that if, using the first reduction, we are able to remove all the instances of the assumption $[a]\mathtt{H}^{\forall\alpha\mathsf{P}} : \forall\alpha^{\mathtt{N}}\mathsf{P}$ in u, then the assumption is unnecessary and the proof term $u \parallel_a v$ may be simplified to u. In this case the exceptional part v of $u \parallel_a v$ is never used.
3. The third EM_1-reduction: $u \parallel_a v \mapsto v[a := n]$, if $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}n$ occurs in u and $\mathsf{P}[n/\alpha] \equiv \mathtt{False}$, says that if we check a closed instance $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}n : \mathsf{P}[n/\alpha]$ of the assumption $\forall\alpha^{\mathtt{N}}\mathsf{P}$, and we find that the assumption is wrong, then we raise in u the exception n and we start the exceptional part $v[a := n]$ of $u \parallel_a v$. Raising an exception is a non-deterministic operation (we may have two or more exceptions to choose) and has no effect outside $u \parallel_a v$.

We claim that the reductions satisfy subject reduction: if $\Gamma \vdash t : A$ and $t \mapsto u$ then $\Gamma \vdash t : A$. The proof is by induction over t. For the reduction rule $u \parallel_a v \mapsto u$ we use the fact that a is not free in u and the Thinning rule. For the reduction rule $u \parallel_a v \mapsto v[a := n]$ we use the fact that a is not free in $v[a := n]$ and Thinning rule again.

As usual, neutral terms are terms that are not "values", and need to be further computed. We also introduce the important 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 hypotheses on which its correctness depends.

▶ **Definition 3** (Neutrality, Quasi-Closed terms)**.**
1. An untyped 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 $[a]\mathtt{H}^{\forall a\mathsf{P}}$ or $u \parallel_a v$.

2. If t is an untyped proof term which contains as free variables only EM_1-hypothesis variables $a_1, \ldots, a_n$, such that each occurrence of them is of the form $[a_i]\mathtt{H}^{\forall\alpha \mathsf{P}_i}$ for some P_i, then t is said to be *quasi-closed*.

Reduction Rules for HA

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

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

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

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

$$\mathsf{R}uv0 \mapsto u$$

$$\mathsf{R}uv(\mathsf{S}n) \mapsto vn(\mathsf{R}uvn), \ \text{for each numeral } n$$

Permutation Rules for EM_1

$$(u \parallel_a v)w \mapsto uw \parallel_a vw, \ \text{if } a \text{ does not occur free in } w$$

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

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

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

Reduction Rules for EM_1

$$([a]\mathtt{H}^{\forall\alpha\mathsf{P}})n \mapsto \mathtt{True}, \ \text{if } \mathsf{P}[n/\alpha] \text{ is } \textit{closed} \text{ and } \mathsf{P}[n/\alpha] \equiv \mathtt{True}$$

$$u \parallel_a v \mapsto u, \ \text{ if } a \text{ does not occur free in } u$$

$$u \parallel_a v \mapsto v[a := n], \ \text{ if } [a]\mathtt{H}^{\forall\alpha\mathsf{P}} n \text{ occurs in } u, \ \mathsf{P}[n/\alpha] \text{ is } \textit{closed} \text{ and } \mathsf{P}[n/\alpha] \equiv \mathtt{False}$$

Figure 2 Reduction Rules for HA + EM_1

3 A Realizability interpretation for $\mathsf{HA} + \mathsf{EM}_1$

In this section we define a realizability semantics for $\mathsf{HA} + \mathsf{EM}_1$, in which realizers may be interpreted as algorithms learning by trial and error a correct value. With respect to the Interactive realizability semantics in [2], the main difference is that we have no formal notion of knowledge state here. Informally, the counterpart of a knowledge state here would be the set of the free EM_1 hypothesis variables occurring in a term and the collection of all assignments $[a := n]$ produced by some reduction $u \parallel_a v \mapsto v[a := n]$ performed in the computation of the term.

Realizers will be deduced to be strongly normalizing terms, and the soundness of this realizability semantics will have strong normalization as a corollary. As in [21], realizers may be untyped terms, and also quasi-closed. With respect to the usual notion of intuitionistic realizability, there is a special case for atomic formulas, and one special case $t = u \parallel_a v$ for the connectives $\vee, \exists$.

▶ **Definition 4** (Realizability for $\mathsf{HA} + \mathsf{EM}_1$). Assume t is a *quasi-closed* term in the grammar of untyped proof terms of $\mathsf{HA} + \mathsf{EM}_1$ and C is a *closed* formula. We define the relation $t \Vdash C$ by induction on C and for each fixed formula by a generalized inductive definition.

1. $t \Vdash \mathsf{P}$ if and only if one of the following holds:

i) $t \in \mathsf{PNF}$ and $\mathsf{P} \equiv \mathtt{False}$ implies t contains a subterm $[a]\mathtt{H}^{\forall\alpha\mathsf{Q}} n$ with $\mathsf{Q}[n/\alpha] \equiv \mathtt{False}$;

ii) $t \notin \mathsf{NF}$ and for all t', $t \mapsto t'$ implies $t' \Vdash \mathsf{P}$

2. $t \Vdash A \wedge B$ if and only if $\pi_0 t \Vdash A$ and $\pi_1 t \Vdash B$

3. $t \Vdash A \to B$ if and only if for all u, if $u \Vdash A$, then $tu \Vdash B$

4. $t \Vdash A \vee B$ if and only if one of the following holds:

i) $t = \iota_0(u)$ and $u \Vdash A$ or $t = \iota_1(u)$ and $u \Vdash B$;

ii) $t = u \parallel_a v$ and $u \Vdash A \vee B$ and $v[a := m] \Vdash A \vee B$ for every numeral m;

iii) $t \notin \mathsf{NF}$ is neutral and for all t', $t \mapsto t'$ implies $t' \Vdash A \vee B$.

5. $t \Vdash \forall \alpha^{\mathtt{N}} A$ if and only if for every closed term n of $\mathcal{L}$, $tn \Vdash A[n/\alpha]$

6. $t \Vdash \exists \alpha^{\mathtt{N}} A$ if and only if one of the following holds:

i) $t = (n, u)$ for some numeral n and $u \Vdash A[n/\alpha]$;

ii) $t = u \parallel_a v$ and $u \Vdash \exists \alpha^{\mathtt{N}} A$ and $v[a := m] \Vdash \exists \alpha^{\mathtt{N}} A$ for every numeral m;

iii) $t \notin \mathsf{NF}$ is neutral and for all t', $t \mapsto t'$ implies $t' \Vdash \exists \alpha^{\mathtt{N}} A$.

► Remark. A realizer is a quasi-closed term, which is interpreted as a program which has made hypotheses in order to decide some instances of EM_1. Its free EM_1 hypothesis variables do not influence the evolution of the term; they represent the assumptions on which the correctness of the computation depends, and they may raise an exception when the term is placed in a context of the form $u \parallel_a v$.

The definition of the realizability relation for the negative connectives $\wedge, \to, \forall$ is standard and it determines the notion of *test*, that is, the kind of input that must be provided to the realizer.

The definition of the realizability relation for the positive connectives $\vee, \exists$ determines the notion of *answer*. We shall see in the crucial Proposition 2 that indeed every realizer *does* provide an answer, under the form of *prediction* (a possibly unsafe answer): a realizer of $A \vee B$ normalizes to a term containing a realizer of A or a realizer of B and a realizer of $\exists \alpha^{\mathtt{N}} A$ normalizes to a term containing a realizer of $A[n/\alpha]$. However, these realizers are only quasi-closed, therefore their correctness depends on extra hypotheses and is not guaranteed: only in the case of closed realizers and of Σ_1^0-formulas we will prove a true disjunction property and a true witness property. The *style* of the definition of realizability for $A \vee B$, $\exists \alpha^{\mathtt{N}} A$ is inspired from Prawitz strong validity [26] and its main feature is that it depends not only on the formula, but also *on the shape of the term*; since it is an inductive definition, a term is a realizer if one can deduce it by means of a finite number of applications of the three subclauses i), ii), iii) of the definition. We observe that the base case i) of the definition is the one of intuitionistic realizability, even if we are in a classical setting: the deep reason of this phenomenon is that in the definition of $u \parallel_a v \Vdash A \vee B$, even if u may contain an hypothesis term $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}$ that becomes free, this term does not "stop" the computation inside u, and u can nevertheless realize $A \vee B$, i.e. reach eventually a form $\iota_i(w)$, after steps of normalization (applications of iii)) or at the end of whatever paths one has followed by applications of ii).

In the case of an atomic formula Q, the definition is analogous to the one of Interactive realizability (see [3] for many intuitions): a proof-term should represent a proof made only of Post-rules (a calculation), possibly with the aid of some hypothesis $\forall\alpha^{\mathtt{N}}\mathsf{P}$; if the formula Q is false, than a counterexample to some hypothesis should be contained in the realizer.

▶ **Example 5** (Realizer of the Excluded Middle)**.** Any closed instance

$$\forall\alpha^{\mathtt{N}}\mathsf{P} \vee \exists\alpha^{\mathtt{N}}\mathsf{P}^{\perp}$$

of EM_1 is provable in $\mathsf{HA} + \mathsf{EM}_1$ by a straightforward application of the EM_1-rule. It shall then be a consequence of the Adequacy Theorem 7 that any instance of EM_1 is realizable. It is however instructive to construct and examine right now a realizer. We define:

$$\mathsf{E}_{\mathsf{P}} := \iota_0([a]\mathtt{H}^{\forall\alpha\mathsf{P}}) \parallel_a \iota_1([a]\mathtt{W}^{\exists\alpha\mathsf{P}^{\perp}})$$

This realizer first tries with $\forall\alpha^{\mathtt{N}}\mathsf{P}$, and if some exception is raised, switches to $\exists^{\mathtt{N}}\alpha\mathsf{P}^{\perp}$. In order to show that

$$\mathsf{E}_{\mathsf{P}} \Vdash \forall\alpha^{\mathtt{N}}\mathsf{P} \vee \exists\alpha^{\mathtt{N}}\mathsf{P}^{\perp}$$

by definition 4 of realizability, we have to prove:

1. $[a]\mathtt{H}^{\forall\alpha\mathsf{P}} \Vdash \forall\alpha^{\mathtt{N}}\mathsf{P}$*, that is, for all numerals* n*,* $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}n \Vdash \mathsf{P}[n/\alpha]$. $\mathsf{P}[n/\alpha]$ is closed because we assumed $\forall\alpha^{\mathtt{N}}\mathsf{P}$ closed. If $\mathsf{P}[n/\alpha] \equiv \mathtt{True}$ then $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}n \mapsto \mathtt{True}$, and $\mathtt{True} \Vdash \mathsf{P}[n/\alpha]$ by definition 4.1.(i), therefore $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}n \Vdash \mathsf{P}[n/\alpha]$ by definition 4.1.(ii). If $\mathsf{P}[n/\alpha] \equiv \mathtt{False}$ then $[a]\mathtt{H}^{\forall\alpha\mathsf{P}}n \Vdash \mathsf{P}[n/\alpha]$ by definition 4.1.(i).

2. *for all numerals* n*,* $[a]\mathtt{W}^{\exists\alpha\mathsf{P}^{\perp}}[a := n] \Vdash \exists\alpha^{\mathtt{N}}\mathsf{P}^{\perp}$. By definition 2, this amounts to show that $(n, \mathtt{True}) \Vdash \exists\alpha^{\mathtt{N}}\mathsf{P}^{\perp}$, when $\mathsf{P}[n/\alpha] \equiv \mathtt{False}$, that is $\mathtt{True} \Vdash \mathsf{P}^{\perp}[n/\alpha]$, and that $(n, [a]\mathtt{H}^{\forall\alpha\,\alpha=0}\mathsf{S}0) \Vdash \exists\alpha^{\mathtt{N}}\mathsf{P}^{\perp}$ otherwise, that is $[a]\mathtt{H}^{\forall\alpha\,\alpha=0}\mathsf{S}0 \Vdash \mathsf{P}^{\perp}[n/\alpha]$. In the first case we have $\mathsf{P}^{\perp}[n/\alpha] \equiv \mathtt{True}$, in the second one the realizer contains an occurrence of $[a]\mathtt{H}^{\forall\alpha\,\alpha=0}\mathsf{S}0$, having $(\alpha = 0)[\alpha/\mathsf{S}0] \equiv \mathtt{False}$. In both case we apply definition 4.1.(i).

4 Basic Properties of Realizers

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

▶ **Definition 6.** Extending the approach of [9], we define four properties **(CR1)**, **(CR2)**, **(CR3)**, **(CR4)** of realizers t of a formula A plus an inhabitation property **(CR5)** for A:

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

(CR2) If $t \Vdash A$ and $t \mapsto^* t'$, then $t' \Vdash A$.

(CR3) If $t \notin \mathsf{NF}$ is neutral and for every t', $t \mapsto t'$ implies $t' \Vdash A$, then $t \Vdash A$.

(CR4) If $t = u \parallel_a v$, $u \Vdash A$ and $v[a := m] \Vdash A$ for every numeral m, then $t \Vdash A$.

(CR5) There is a u such that $u \Vdash A$.

All properties listed above hold.

▶ Proposition 1. Every term t has the properties **(CR1)**, **(CR2)**, **(CR3)**, **(CR4)** and the inhabitation property **(CR5)** holds.

As we pointed out in the introduction, we cannot prove that any realizer of a disjunction or an existential contains a *correct witness*, but we may prove some weakening of this property: in some sense, surprisingly, also classical logic enjoys the disjunction and numerical existence properties. Namely, a realizer of $A \vee B$ contains a realizer of A or a realizer of B and a realizer of $\exists \alpha^{\mathtt{N}} A$ contains a realizer of $A[n/\alpha]$. The point is that n is not necessarily a true witness, but rather a *prediction* based on the universal assumptions contained in the realizer.

▶ Proposition 2 (Weak Disjunction and Numerical Existence Properties).

1. Suppose $t \Vdash A \vee B$. Then either $t \mapsto^* \mathcal{EM}[\iota_0(u)]$ and $u \Vdash A$ or $t \mapsto^* \mathcal{EM}[\iota_1(u)]$ and $u \Vdash B$.
2. Suppose $t \Vdash \exists \alpha^{\mathtt{N}} A$. Then $t \mapsto^* \mathcal{EM}[(n, u)]$ for some numeral n such that $u \Vdash A[n/\alpha]$.

Proof.

1. Since $t \in \mathsf{SN}$ by **(CR1)**, let t' be such that $t \mapsto^* t' \in \mathsf{NF}$. By **(CR2)**, $t' \Vdash A \vee B$. If $t' = \iota_0(u)$, we are done. The only possibility left is that $t' = v \parallel v_1 \parallel v_2 \ldots \parallel v_n$, with v not of the form $w_0 \parallel w_1$. By definition 4.4.(ii) we have $v \Vdash A \vee B$, and since v is normal and not of the form $w_0 \parallel w_1$, by definition 4.4.(i) we have either $v = \iota_0(u)$, with $u \Vdash A$, or $v = \iota_1(u)$, with $u \Vdash B$.
2. Similar to 1.

◀

We observe that in a realizer $v \parallel_{a_1} v_1 \parallel_{a_2} v_2 \ldots \parallel_{a_n} v_n$ of $A \vee B$, the further we move on the left, the larger is the set of hypotheses becoming free. This is indeed the price payed to construct a realizer of A or B, which is contained in v: hypotheses have to be made.

The next task is to prove that all introduction and elimination rules of $\mathsf{HA} + \mathsf{EM}_1$ define a realizer from a list of realizers for all premises. In some case this is true by definition of realizer, we list below some non-trivial cases we have to prove.

▶ Proposition 3.

1. If for every $t \Vdash A$, $u[t/x] \Vdash B$, then $\lambda x\, u \Vdash A \to B$.
2. If for every closed term m of $\mathcal{L}$, $u[m/\alpha] \Vdash B[m/\alpha]$, then $\lambda \alpha\, u \Vdash \forall \alpha^{\mathtt{N}} B$.
3. If $u \Vdash A_0$ and $v \Vdash A_1$, then $\pi_i \langle u, v \rangle \Vdash A_i$.
4. If $w_0[x_0.u_0, x_1.u_1] \Vdash C$ and for all numerals n, $w_1[x_0.u_0, x_1.u_1][a := n] \Vdash C$, then $(w_0 \parallel_a w_1)[x_0.u_0, x_1.u_1] \Vdash C$.
5. If $t \Vdash A_0 \vee A_1$ and for every $t_i \Vdash A_i$ it holds $u_i[t_i/x_i] \Vdash C$, then $t[x_0.u_0, x_1.u_1] \Vdash C$.
6. If $t \Vdash \exists \alpha^{\mathtt{N}} A$ and for every term n of $\mathcal{L}$ and $v \Vdash A[n/\alpha]$ it holds $u[n/\alpha][v/x] \Vdash C$, then $t[(\alpha, x).u] \Vdash C$.

5 The Adequacy Theorem

In this section we prove that the realizability semantics we defined in §3 is sound for $\mathsf{HA}+\mathsf{EM}_1$, and we derive strong normalization as a corollary. The witness property for Σ^0_1-formulas, instead, may be derived directly from the basic properties of realizers (§4).

▶ **Theorem 7** (Adequacy Theorem). *Suppose that* $\Gamma \vdash w : A$ *in the system* $\mathsf{HA} + \mathsf{EM}_1$*, with*

$$\Gamma = x_1 : A_1, \ldots, x_n : A_n, a_1 : \exists \alpha_1^{\mathtt{N}} \mathsf{P}_1^{\perp}, \ldots, a_m : \exists \alpha_m^{\mathtt{N}} \mathsf{P}_m^{\perp}, b_1 : \forall \alpha_1^{\mathtt{N}} \mathsf{Q}_1, \ldots, b_l : \forall \alpha_l^{\mathtt{N}} \mathsf{Q}_l$$

and that the free variables of the formulas occurring in Γ *and* A *are among* $\alpha_1, \dots, \alpha_k$*. For all closed terms* $r_1, \dots, r_k$ *of* $\mathcal{L}$*, if there are terms* $t_1, \dots, t_n$ *such that*

$$\textit{for } i = 1, \dots, n,\ t_i \Vdash A_i[r_1/\alpha_1 \cdots r_k/\alpha_k]$$

then

$$w[t_1/x_1 \cdots t_n/x_n\ r_1/\alpha_1 \cdots r_k/\alpha_k\ a_1 := i_1 \cdots a_m := i_m] \Vdash A[r_1/\alpha_1 \cdots r_k/\alpha_k]$$

for every numerals $i_1, \dots, i_m$*.*

▶ **Corollary 8** (Strong Normalization of HA+EM1). *All terms of* $\mathsf{HA} + \mathsf{EM}_1$ *are strongly normalizing.*

Proof. From Theorem 7 and **(CR5)** we derive that for all proof-terms $t : A$ we have some substitution t' such that $t' \Vdash A$. From **(CR1)** we conclude that t' is strongly normalizing: as a corollary, t itself is strongly normalizing. ◀

Our last task is to prove that all proofs of simply existential statements include a witness.

▶ **Theorem 9** (Normal Form Property and Existential Witness Extraction). *Suppose* t *is closed,* $t \Vdash \exists \alpha^{\mathtt{N}} \mathsf{P}$ *and* $t \mapsto^* t' \in \mathsf{NF}$*. Then* $t' = (n, u)$ *for some numeral* n *such that* $\mathsf{P}[n/\alpha] \equiv \mathtt{True}$*.*

Proof. By proposition 2, there is some numeral n such that $t' = \mathcal{EM}[(n, u)]$ and $u \Vdash \mathsf{P}[n/\alpha]$. So

$$t' = (n, u) \parallel_{a_1} v_1 \parallel_{a_2} v_2 \dots \parallel_{a_m} v_m$$

Since t' is closed, u is quasi-closed and all its free variables are among $a_1, a_2, \dots, a_m$. We observe that u must be closed. Otherwise, by definition 4.1.(i) and $u \Vdash \mathsf{P}[n/\alpha]$ we deduce that $u \in \mathsf{PNF}$, and thus u should contain a subterm $[a_i]\mathtt{H}^{\forall \alpha \mathsf{Q}} n$; moreover, $\mathsf{Q}[n/\alpha] \equiv \mathtt{False}$ otherwise u would not be normal; but then we would have either $m \neq 0$ and $t' \notin \mathsf{NF}$ because $t' \mapsto v_1[a_1 := n] \parallel_{a_2} v_2 \dots \parallel_{a_m} v_m$, or $m = 0$ and t' non-closed. Since u is closed, we obtain $t' = (n, u)$, for otherwise $t' \mapsto (n, u) \parallel_{a_2} v_2 \dots \parallel_{a_m} v_m$ and $t' \notin \mathsf{NF}$. Since $u \Vdash \mathsf{P}[n/\alpha]$, by definition 4.1.(i) it must be $\mathsf{P}[n/\alpha] \equiv \mathtt{True}$. ◀

By the Adequacy Theorem 7 and Theorem 9, whenever $\mathsf{HA} + \mathsf{EM}_1$ proves a closed formula of the shape $\forall \alpha_1^{\mathtt{N}} \dots \forall \alpha_k^{\mathtt{N}} \exists \beta^{\mathtt{N}} \mathsf{P}$, one can extract a realizer t with the property that, for every numerals $n_1, \dots, n_k$, there is some numeral n such that $t n_1 \dots n_k \mapsto^* (n, \mathtt{True})$ and $\mathsf{P}[n_1/\alpha_1 \cdots n_k/\alpha_k\, n/\beta] \equiv \mathtt{True}$. For example, from a proof of $\forall \alpha_1^{\mathtt{N}} \forall \alpha_2^{\mathtt{N}} \exists \beta^{\mathtt{N}} \mathsf{add}(\alpha_1, \alpha_2, \beta)$, one can extract a term computing the sum of natural numbers, even if the proposition has been proved classically.

6 Conclusions

From the point of view of classical Curry-Howard correspondence, the main contribution of this paper is a new decomposition of the EM_1 reduction rules in terms of delimited exceptions and permutation rules. The expert may at this point have noticed that some deterministic restriction of our conversions may be quite directly simulated in $\lambda\mu$-calculus and, less directly, in Krivine's λ_c-calculus. However, as it is quite often the case in proof theory, a variation in the rules of a system may be crucial to gain better results and understanding. In our case, with our approach we obtain several new results.

- *Markov's Principle and Restricted* EM_1. The mechanism of delimited exceptions allows to obtain quite refined results about systems containing Markov's principle, showing directly that its addition on top of intuitionistic logic preserves the disjunction and numerical existence properties [16]. Of course, Markov's principle is provable in $\mathsf{HA} + \mathsf{EM}_1$, by the most restricted version of the EM_1 rules, where the conclusion of the rule must be a Σ^1_0-formula. We shall show in a future paper that also our system enjoys the disjunction and numerical existence properties, when it is only allowed to use the restricted excluded middle sufficient to prove Markov's principle.
- *Extension of Prawitz validity to classical proofs.* The double negation is in some sense hardwired in the $\lambda\mu$ and in the λ_c calculi. As the cognoscenti know, this forces Krivine's realizability of a formula A for these calculi to have the form $\neg A \to \bot$, where $\neg A$ is the type of stacks and $\bot$ is interpreted by $\perp\!\!\!\perp$. Loosely speaking, in this way double negation elimination becomes a tautology: $(\neg\neg A) \to \neg A \to \bot$. Our priority is instead given to EM_1, and our reduction rules allow to extend an introductions-based Prawitz validity to a classical system. Such a result would not have been possible in the context of $\lambda\mu$ or λ_c.
- *Weak disjunction and existence properties for realizability.* Thanks to the essentially positive flavor of our realizability definition for positive connectives, we have shown (Proposition 2) that our notion of realizability satisfies a remarkable property: a realizer of a disjunction contains a realizer of one of the disjuncts, and a realizer of an existential statement contains a realizer of an instance of it. Similar insights seem not possible to be easily expressed in the framework of $\lambda\mu$-calculus or Krivine's realizability (or at least, similar properties have never been noticed). It is instead the explanation of classical programs as making hypotheses, testing them and learning, that has led to our results: our realizers behave like they do *precisely* because they want to achieve the disjunction and numerical existence properties during computations.

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 $SK1$*, Technical Report, http://hal.inria.fr/hal-00657054.

6 S. Berardi, *An Interactive Realizability Semantics for non-constructive proofs*, Chambery Summer school of Realization, Chambery, 14-17 June, 2011.

`http://www.di.unito.it/~stefano/Berardi-RealizationChambery-13Giugno2011.pdf`

7 S. Berardi, *Some intuitionistic equivalents of classical principles for degree 2 formulas.* Ann. Pure Appl. Logic 139(1-3): 185-200 (2006)

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

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

10 H. Friedman, *Classically and Intuitionistically Provable Recursive Functions*, Lecture Notes in Mathematics, 1978, Volume 669/1978, 21-27.

11 K. Gödel, *Uber eine bisher noch nicht benutzte Erweiterung des finiten Standpunktes*, Dialectica 12, pp. 280-287 (1958).

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

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

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

15 T. Griffin, *A Formulae-as-Type Notion of Control*, Proc. of POPL, 1990.

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

17 U. Kohlenbach, *On uniform weak König's lemma.* Annals of Pure and Applied Logic, 114(1-3) (2002).

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

19 J.-L. Krivine, *Lambda-calcul types et modèles*, Studies in Logic and Foundations of Mathematics (1990) 1–176. Masson, Paris.

20 J.-L. Krivine, *Dependent Choiche, "Quote" and the Clock*, Theoretical Computer Science 308(1-3), 2003, 259–276.

21 J.-L. Krivine, *Classical Realizability.* In Interactive models of computation and program behavior. Panoramas et synthèses , 2009, 197–229. Société Mathématique de France.

22 J.-L. Krivine, *Realizability Algebras II: new models of ZF + DC*, Logical Methods in Computer Science, 2012.

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

24 A. Miquel, *Existential witness extraction in classical realizability and via a negative translation.* Logical Methods in Computer Science 7(2) (2011)

25 M. Parigot, *Lambda-My-Calculus: An Algorithmic Interpretation of Classical Natural Deduction.* LPAR 1992: 190-201.

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

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

28 J. von Plato: *A Constructive Approach to Sylvester's Conjecture.* J. UCS 11(12): 2165-2178 (2005)

A Proofs of the Main Theorems

Proof of Proposition 1. By induction on C. For **(CR5)** we prove, in particular that $\mathsf{c}^C \Vdash C$, where c^C is defined by induction on C as follows: $\mathsf{c}^{\mathsf{P}} := [a]\mathtt{H}^{\forall\alpha\, \alpha=0}\mathsf{S}0$; $\mathsf{c}^{A\wedge B} := \langle \mathsf{c}^A, \mathsf{c}^B\rangle$; $\mathsf{c}^{A\vee B} := \iota_0(\mathsf{c}^A)$; $\mathsf{c}^{A\to B} := \lambda\_.\mathsf{c}^B$; $\mathsf{c}^{\exists\alpha^{\mathtt{N}} A} := (0, \mathsf{c}^{A[0/\alpha]})$; $\mathsf{c}^{\forall\alpha^{\mathtt{N}} A} := \lambda\_.\mathsf{c}^{A[0/\alpha]}$.

- $C = \mathsf{P}$ is atomic.

  (CR1). By induction on the definition of $t \Vdash \mathsf{P}$. If $t \in \mathsf{PNF}$, then $t \in \mathsf{SN}$. If $t \notin \mathsf{NF}$, then $t \mapsto t'$ implies $t' \Vdash \mathsf{P}$ and thus by induction hypothesis $t' \in \mathsf{SN}$; so $t \in \mathsf{SN}$.

  (CR2). Suppose $t \Vdash \mathsf{P}$. It suffices to assume that $t \mapsto t'$ and show that $t' \Vdash \mathsf{P}$. The case $t \in \mathsf{PNF}$ cannot occur, since t would be normal. If $t \notin \mathsf{NF}$ is neutral, then by definition of

$t \Vdash \mathsf{P}$ we obtain $t' \Vdash \mathsf{P}$.

(CR3) is trivially true by definition of $t \Vdash \mathsf{P}$.

(CR4) Suppose $u \Vdash \mathsf{P}$ and for all numerals n, $v[a := n] \Vdash \mathsf{P}$. Since by **(CR1)**, $u, v \in \mathsf{SN}$, in order to show that $u \parallel_a v \Vdash \mathsf{P}$, we can proceed by induction on the sum of the heights of the reduction trees of u and v. We first show that $u \parallel_a v \notin \mathsf{NF}$. If a does not occur free in u, then surely $u \parallel_a v \notin \mathsf{NF}$. Suppose then a occurs free in u . If $u \notin \mathsf{NF}$, we are done; suppose than $u \in \mathsf{NF}$. Since $u \Vdash \mathsf{P}$, then $u \in \mathsf{PNF}$. Since a occurs free in u, u contains at least a subterm of the form $[a]\mathtt{H}^{\forall \alpha \mathsf{Q}} n$, with $\mathsf{Q}[n/\alpha] \equiv \mathtt{False}$. We conclude, $u \parallel_a v \notin \mathsf{NF}$. By definition or realizability, we now have to prove that if $u \parallel_a v \mapsto z$, then $z \Vdash \mathsf{P}$. If $z = u$ or $z = v[a := m]$ for some numeral m, we obtain the thesis by hypothesis. If $z = u' \parallel_a v$, with $u \mapsto u'$, then by **(CR2)**, $u' \Vdash \mathsf{P}$. So $u' \parallel_a v \Vdash \mathsf{P}$ by induction hypothesis. If $z = u \parallel_a v'$, with $v \mapsto v'$, then for every numeral n, $v[a := n] \mapsto v'[a := n]$, and thus by **(CR2)** $v'[a := n] \Vdash \mathsf{P}$. So $u \parallel_a v' \Vdash \mathsf{P}$ by induction hypothesis.

(CR5). We have that $[a]\mathtt{H}^{\forall \alpha\, \alpha = 0}\mathsf{S}0 \Vdash \mathsf{P}$.

- $C = A \to B$.

  (CR1). Suppose $t \Vdash A \to B$. By induction hypothesis **(CR5)**, there is an u such that $u \Vdash A$; therefore, $tu \Vdash B$. By induction hypothesis **(CR1)**, $tu \in \mathsf{SN}$ and thus $t \in \mathsf{SN}$.

  (CR2) and **(CR3)** are proved as in [9].

  (CR4). Suppose $u \Vdash A \to B$ and $v[a := n] \Vdash A \to B$ for every numeral n. Let $t \Vdash A$. We show by induction on the sum of the heights of the reduction trees of u, v, t (they are all in SN by **(CR1)**) that $(u \parallel_a v)t \Vdash B$. By induction hypothesis **(CR3)**, it is enough to assume $(u \parallel_a v)t \mapsto z$ and show $z \Vdash B$. If $z = ut$ or $v[a := n]t$, we are done. If $z = (u' \parallel_a v)t$ or $z = (u \parallel_a v')t$ or $(u \parallel_a v)t'$, with $u \mapsto u'$, $v \mapsto v'$ and $t \mapsto t'$, we obtain $z \Vdash B$ by **(CR2)** and induction hypothesis. If $z = (ut \parallel_a vt)$, by induction hypothesis **(CR4)**, $z \Vdash B$.

  (CR5). By induction hypothesis **(CR5)**, $\mathsf{c}^B \Vdash B$. We want to show that $\lambda\_.\mathsf{c}^B \Vdash A \to B$. Suppose $t \Vdash A$: we have to show that $(\lambda\_.\mathsf{c}^B)t \Vdash B$. We proceed by induction on the height of the reduction tree of t (by **(CR1)**, $t \in \mathsf{SN}$). By induction hypothesis **(CR3)**, it is enough to assume $(\lambda\_.\mathsf{c}^B)t \mapsto z$ and show $z \Vdash B$. If $z = \mathsf{c}^B$, we are done. If $z = (\lambda\_.\mathsf{c}^B)t'$, with $t \mapsto t' \Vdash A$ (by **(CR2)**), we obtain $z \Vdash B$ by induction hypothesis. There are no other cases, for $\mathsf{c}^B \in \mathsf{NF}$ by construction.

- $C = \forall \alpha^{\mathtt{N}} A$ or $C = A \wedge B$. Similar to the case $C = A \to B$.

- $C = A_0 \vee A_1$.

  (CR1) By induction on the definition of $t \Vdash A_0 \vee A_1$. If $t = \iota_i(u)$, then $u \Vdash A_i$, and by induction hypothesis **(CR1)**, $u \in \mathsf{SN}$; therefore, $t \in \mathsf{SN}$. If $t \notin \mathsf{NF}$ is neutral, then $t \mapsto t'$ implies $t' \Vdash A_0 \vee A_1$ and thus $t' \in \mathsf{SN}$ by induction hypothesis; therefore, $t \in \mathsf{SN}$. Suppose then $t = u \parallel_a v$. Since $u \Vdash A_0 \vee A_1$ and for all numerals n, $v[a := n] \Vdash A_0 \vee A_1$, we have by induction hypothesis $u \in \mathsf{SN}$ and for all numerals n, $v[a := n] \in \mathsf{SN}$. But these last two conditions are easily seen to imply $u \parallel_a v \in \mathsf{SN}$

(CR2). Suppose $t \Vdash A_0 \vee A_1$. It suffices to assume that $t \mapsto t'$ and show that $t' \Vdash A_0 \vee A_1$. We proceed by induction on the definition of $t \Vdash A_0 \vee A_1$. If $t = \iota_i(u)$, then $t' = \iota_i(u')$, with $u \mapsto u'$. By definition of $t \Vdash A_0 \vee A_1$, we have $u \Vdash A_i$. By induction hypothesis **(CR2)**, $u' \Vdash A_i$ and thus $t' \Vdash A_0 \vee A_1$. If $t \notin \mathsf{NF}$ is neutral, by definition of $t \Vdash A_0 \vee A_1$, we obtain that $t' \Vdash A_0 \vee A_1$. If $t = u \parallel_a v$, with $u \Vdash A_0 \vee A_1$ and for all numerals n, $v[a := n] \Vdash A_0 \vee A_1$. If $t' = u$ or $t' = v[a := m]$, we are done. If $t' = u' \parallel_a v$, with $u \mapsto u'$, then by induction hypothesis, $u' \Vdash A_0 \vee A_1$. So $u' \parallel_a v \Vdash A_0 \vee A_1$ by definition. If $t' = u \parallel_a v'$, with $v \mapsto v'$, then for every numeral n, $v[a := n] \mapsto v'[a := n]$ and thus by induction hypothesis $v'[a := n] \Vdash A_0 \vee A_1$. So $u \parallel_a v' \Vdash A_0 \vee A_1$ by definition.

(CR3) and **(CR4)** are trivial.

(CR5). By induction hypothesis **(CR5)**, $\mathsf{c}^{A_0} \Vdash A_0$. Thus $\iota_0(\mathsf{c}^{A_0}) \Vdash A_0 \vee A_1$.

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

◀

Proof of Proposition 3.

1. As in [9].
2. As in [9].
3. As in [9].

4. We may assume a does not occur in u_0, u_1. By hypothesis, $w_0[x_0.u_0, x_1.u_1] \Vdash C$ and for every numeral n, $w_1[x_0.u_0, x_1.u_1][a := n] \Vdash C$. By **(CR1)**, in order to show $w_0 \parallel_a w_1[x_0.u_0, x_1.u_1] \Vdash C$, we may proceed by induction on the sum of the sizes of the reduction trees of w_0, w_1, u_0, u_1. By **(CR3)**, it then suffices to assume that $w_0 \parallel_a w_1[x_0.u_0, x_1.u_1] \mapsto z$ and show $z \Vdash C$. If $z = w_0[x_0.u_0, x_1.u_1]$ or $w_1[a := n][x_0.u_0, x_1.u_1]$ for some numeral n, we are done. If $z = w_0' \parallel_a w_1[x_0.u_0, x_1.u_1]$ or $z = w_0 \parallel_a w_1'[x_0.u_0, x_1.u_1]$ or $z = w_0 \parallel_a w_1[x_0.u_0', x_1.u_1]$ or $z = w_0 \parallel_a w_1[x_0.u_0, x_1.u_1']$, with $w_i \mapsto w_i'$ and $u_i \mapsto u_i'$, then by **(CR2)** we can apply the induction hypothesis and obtain $z \Vdash C$. If
$$z = (w_0[x_0.u_0, x_1.u_1]) \parallel_a (w_1[x_0.u_0, x_1.u_1])$$
then $z \Vdash C$ by **(CR4)**.

5. Suppose $t \Vdash A_0 \vee A_1$ and for every $t_i \Vdash A_i$ it holds $u_i[t_i/x_i] \Vdash C$. In order to show $t[x_0.u_0, x_1.u_1] \Vdash C$, we reason by induction of the definition of $t \Vdash A_0 \vee A_1$. Since by **(CR5)** there are v_0, v_1 such that $v_i \Vdash A_i$, we have $u_i[v_i/x_i] \Vdash A_i$, and thus by **(CR1)**, $u_i[v_i/x_i] \in \mathsf{SN}$ and $t \in \mathsf{SN}$. We have three cases:

   - $t = \iota_i(u)$. Then $u \Vdash A_i$. We want to show that for every $u' \Vdash A_i$, $\iota_0(u')[x_0.u_0, x_1.u_1] \Vdash C$. By **(CR3)**, it suffices to assume that $\iota_0(u)[x_0.u_0, x_1.u_1] \mapsto z$ and show $z \Vdash C$. We reason by induction on the sum of the sizes of the reduction trees of u, u_0, u_1. If $z = \iota_i(u')[x_0.u_0, x_1.u_1]$ or $z = t[x_0.u_0', x_1.u_1]$ or $z = t[x_0.u_0, x_1.u_1']$, with $u \mapsto u'$ and $u_i \mapsto u_i'$, then by **(CR2)** we can apply the induction hypothesis and obtain $z \Vdash C$. If $z = u_i[u/x_i]$, since $u \Vdash A_i$, we obtain $z \Vdash C$.

- $t = w_0 \parallel_a w_1$. By induction hypothesis $w_0[x_0.u_0, x_1.u_1] \Vdash C$ and for all numerals n, $w_1[a := n][x_0.u_0, x_1.u_1] \Vdash C$. By 4., $w_0 \parallel_a w_1[x_0.u_0, x_1.u_1] \Vdash C$.

- $t \notin \mathsf{NF}$ is neutral. We reason by induction on the sum of the sizes of the reduction trees of u_0, u_1. By **(CR3)**, it suffices to assume that $t[x_0.u_0, x_1.u_1] \mapsto z$ and show $z \Vdash C$. If $z = t'[x_0.u_0, x_1.u_1]$, we apply the (main) induction hypothesis and obtain $z \Vdash C$. If $z = t[x_0.u_0', x_1.u_1]$ or $z = t[x_0.u_0, x_1.u_1']$, with $u \mapsto u'$ and $u_i \mapsto u_i'$, then by **(CR2)** we can apply the induction hypothesis and obtain $z \Vdash C$.

6. Analogous to 5.

◀

Proof of Theorem 7. Notation: for any term v and formula B, we denote

$$v[t_1/x_1 \cdots t_n/x_n \; r_1/\alpha_1 \cdots r_k/\alpha_k \; a_1 := i_1 \cdots a_m := i_m]$$

with $\overline{v}$ and

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

with $\overline{B}$. We proceed by induction on w and we cover only some significant cases. Consider the last rule in the derivation of $\Gamma \vdash w : A$:

1. If it is the rule $\Gamma \vdash [b_j]\mathtt{H}^{\forall\alpha_j \mathsf{P}_j} : \forall\alpha_j^{\mathtt{N}}\mathsf{P}_j$, then $w = [b_j]\mathtt{H}^{\forall\alpha_j \mathsf{P}_j}$ and $A = \forall\alpha_j^{\mathtt{N}}\mathsf{P}_j$. So $\overline{w} = [b_j]\mathtt{H}^{\forall\alpha_j \overline{\mathsf{P}_j}}$. Let n be any closed term of $\mathcal{L}$. We must show that $\overline{w}n \Vdash \overline{\mathsf{P}_j}[n/\alpha_j]$. We have $[b_j]\mathtt{H}^{\forall\alpha_j \overline{\mathsf{P}_j}}n \in \mathsf{SN}$; moreover, if $[b_j]\mathtt{H}^{\forall\alpha_j \overline{\mathsf{P}_j}}n \mapsto z$, then z is $\mathtt{True}$ and $\overline{\mathsf{P}_j}[n/\alpha_j] \equiv \mathtt{True}$, and thus $z \Vdash \overline{\mathsf{P}_j}[n/\alpha_j]$; if $\mathtt{H}^{\forall\alpha_j \overline{\mathsf{P}_j}}n \in \mathsf{NF}$, then $\overline{\mathsf{P}_j}[n/\alpha_j] \equiv \mathtt{False}$. We conclude $[b_j]\mathtt{H}^{\forall\alpha_j \overline{\mathsf{P}_j}} \Vdash \forall\alpha_j^{\mathtt{N}}\overline{\mathsf{P}_j} = \overline{A}$.

2. If it is the rule $\Gamma \vdash [a_j]\mathtt{W}^{\exists\alpha_j \mathsf{P}_j^{\perp}} : \exists\alpha_j^{\mathtt{N}}\mathsf{P}_j^{\perp}$, then $w = [a_j]\mathtt{W}^{\exists\alpha_j \mathsf{P}_j^{\perp}}$ and $A = \exists\alpha_j^{\mathtt{N}}\mathsf{P}_j^{\perp}$. We have two possibilities. i) $\overline{w} = (i_j, \mathtt{True})$ and $\overline{\mathsf{P}_j}[i_j/\alpha_j] \equiv \mathtt{False}$. But this means that $\overline{w} \Vdash \exists\alpha_j^{\mathtt{N}}\overline{\mathsf{P}_j}^{\perp}$. ii) $\overline{w} = (i_j, [a_j]\mathtt{H}^{\forall\alpha\, \alpha=0}\mathsf{S}0)$. Again, $\overline{w} \Vdash \exists\alpha_j^{\mathtt{N}}\overline{\mathsf{P}_j}^{\perp}$.

3. If it 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 $\overline{u} \Vdash \overline{B}$ and thus $\overline{u} \in \mathsf{SN}$. We conclude $\iota_0(\overline{u}) \Vdash \overline{B} \vee \overline{C} = \overline{A}$.

4. If it 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 $\overline{u} \Vdash \overline{B} \vee \overline{C}$; moreover, for every $t \Vdash \overline{B}$, we have $\overline{w}_1[t/x] \Vdash \overline{B}$ and for every $t \Vdash \overline{C}$, we have $\overline{w}_2[t/y] \Vdash \overline{C}$. By proposition 3, we obtain $\overline{w} = \overline{u}[x.\overline{w}_1, y.\overline{w}_2] \Vdash \overline{C}$.

5. The cases $\exists I$ and $\exists E$ are similar respectively to $\vee I$ and $\vee E$.

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

7. If it is the $\forall I$ rule, then $w = \lambda \alpha u$, $A = \forall \alpha^{\mathtt{N}} B$ 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 any closed term of $\mathcal{L}$; by proposition 3), it is enough to prove that $\overline{u}[t/\alpha] \Vdash \overline{B}[t/\alpha]$, 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

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

8. If it is the induction rule, then $w = \mathsf{R}uvt$, $A = B(t)$, $\Gamma \vdash u : B(0)$ and $\Gamma \vdash v : \forall \alpha^{\mathtt{N}}.B(\alpha) \rightarrow B(\mathsf{S}(\alpha))$. So, $\overline{w} = \mathsf{R}\overline{u}\overline{v}l$, for some numeral $l = \overline{t}$.
We prove that for all numerals n, $\mathsf{R}\overline{u}\overline{v}n \Vdash \overline{B}(n)$. By **(CR3)**, it is enough to suppose that $\mathsf{R}\overline{u}\overline{v}n \mapsto w$ and show that $w \Vdash \overline{B}(n)$. By induction hypothesis $\overline{u} \Vdash \overline{B}(0)$ and $\overline{v}m \Vdash \overline{B}(m) \rightarrow \overline{B}(\mathsf{S}(m))$ for all closed terms m of $\mathcal{L}$. So by **(CR1)**, we can reason by induction on the sum of the sizes of reduction trees of $\overline{u}$ and $\overline{v}$ and the size of m. If $n = 0$ and $w = \overline{u}$, then we are done. If $n = \mathsf{S}(m)$ and $w = \overline{v}m(\mathsf{R}\overline{u}\overline{v}m)$, by induction hypothesis $\mathsf{R}\overline{u}\overline{v}m \Vdash \overline{B}(m)$; therefore, $w \Vdash \overline{B}(\mathsf{S}m)$. If $w = \mathsf{R}u'\overline{v}m$, with $\overline{u} \mapsto u'$, by induction hypothesis $w \Vdash \overline{B}(m)$. We conclude the same if $w = \mathsf{R}\overline{u}v'm$, with $\overline{v} \mapsto v'$.
We thus obtain that $\overline{w} \Vdash \overline{B}(l) = \overline{B(t)}$.

9. If it is the EM_1 rule, then $w = u \parallel_a v$, $\Gamma, a : \forall \alpha^{\mathtt{N}} \mathsf{P} \vdash u : C$ and $\Gamma, a : \exists \alpha^{\mathtt{N}} \mathsf{P}^{\perp} \vdash v : C$ and $A = C$. By induction hypothesis, $\overline{u} \Vdash \overline{C}$ and for all numerals m, $\overline{v}[a := m] \Vdash \overline{C}$. By **(CR4)**, we conclude $\overline{w} = \overline{u} \parallel_a \overline{v} \Vdash \overline{C}$.

10. If it is a Post rule, the case w is $\mathtt{True}$ is trivial, so we may assume $w = \mathsf{r}t_1 \ldots t_n$, $A = \mathsf{P}$ and $\Gamma \vdash t_1 : \mathsf{P}_1, \ldots, \Gamma \vdash t_n : \mathsf{P}_n$. By induction hypothesis, for $i = 1, \ldots, n$, we have $\overline{t}_i \Vdash \overline{\mathsf{P}_i}$. By **(CR1)**, we can argue by induction on the size of the reduction tree of $\overline{w}$. We have two cases. i) $\overline{w} \in \mathsf{NF}$. For $i = 1, \ldots, n$, by theorem 9, we obtain $\overline{t}_i \in \mathsf{PNF}$. Therefore, also $\overline{w} \in \mathsf{PNF}$. Assume now $\overline{\mathsf{P}} \equiv \mathtt{False}$. Then, for some i, $\overline{\mathsf{P}_i} \equiv \mathtt{False}$. Therefore, $\overline{t}_i$ contains a subterm $[a]\mathtt{H}^{\forall \alpha \mathsf{Q}} n$ with $\mathsf{Q}[n/\alpha] \equiv \mathtt{False}$ and thus also $\overline{w}$. We conclude $\overline{w} \Vdash \overline{\mathsf{P}}$. ii) $\overline{w} \notin \mathsf{NF}$. By **(CR3)**, it is enough to suppose $\overline{w} \mapsto z$ and show $z \Vdash \overline{\mathsf{P}}$. We have $z = \mathsf{r}\overline{t}_1 \ldots \overline{t}'_i \ldots \overline{t}_n$, with $\overline{t}_i \mapsto \overline{t}'_i$, and by **(CR2)**, $\overline{t}'_i \Vdash \overline{\mathsf{P}_i}$. By induction hypothesis, $z \Vdash \overline{\mathsf{P}}$.

◀