Interactive realizers. A new approach to program extraction from non constructive proofs

STEFANO BERARDI
Università di Torino
UGO DE'LIGUORO
Università di Torino

We propose a realizability interpretation of a system for quantier free arithmetic which is equivalent to the fragment of classical arithmetic without *nested* quantifiers, called here $\mathbf{EM}_1$-arithmetic. We interpret classical proofs as interactive learning strategies, namely as processes going through several stages of knowledge and learning by interacting with the "nature", represented by the standard interpretation of closed atomic formulas, and with each other. We obtain in this way a program extraction method by proof interpretation, which is faithful w.r.t. proofs, in the sense that it is compositional and that it does not need any translation.

Categories and Subject Descriptors: D.1.1 [**Software**]: Applicative (Functional) Programming; D.1.2 [**Software**]: Automatic Programming; F.1.2 [**Theory of Computation**]: Modes of Computation—*Interactive and reactive computation*; F.4.1 [**Mathematical Logic**]: Lambda calculus and related systems—*Proof Theory*; I.2.6 [**Artificial Intelligence**]: Learning—*Induction*

General Terms: Theory, Languages

Additional Key Words and Phrases: Realizability, Learning in the Limit, Constructive Interpretations of Classical Logic.

1. INTRODUCTION

It is well known that even from a non constructive proof of a Π^0_2 statement $\forall x \exists y A(x, y)$ one can extract an algorithm to compute a non trivial term $t(x)$ such that $\forall x A(x, t(x))$. Extraction techniques fall into two groups: either by cut elimination and proof normalization, or by proof interpretation. We investigate here a new approach to program extraction by proof interpretation, based on realizability and learning (see subsection 1.1 for references).

Kleene's realizers and their subsequent variants are recursive functions that, in case of intuitionistic proofs, directly compute the term $t(x)$. To cope with classical proofs a translation is needed, like Gödel's or Friedman's. Inspired by Coquand's game theoretic interpretation of classical arithmetic and Gold's learning in the limit, we propose a notion of "interactive realizability" which is a direct interpretation of (a restricted class of) classical reasonings, not requiring the translation step.

To illustrate the idea, consider the statement:

$$\exists x. f(x) \leq f(g(x)) \wedge f(x) \leq f(h(x)) \tag{1}$$

where x is in $\mathbb{N}$, and f, g and h are arbitrary total recursive functions. This statement is classically provable, by choosing an n such that $f(n)$ is the minimum in $\mathrm{rng}(f) = \{f(n) \mid n \in \mathbb{N}\}$. Such a proof is essentially non constructive, since computing the minimum of $\mathrm{rng}(f)$ uniformly in f entails decidability of the halting problem. This is not to say that we cannot find an m such that $f(m) \leq f(g(m)) \wedge f(m) \leq f(h(m))$ because, once we know the truth of (1), such an m can be found by minimalization. Such a brute force algorithm has nothing to do with the proof we sketch above; indeed it relies just on the existence of a proof, and could be hardly considered as its computational content.

Author's address: S. Berardi and U. de'Liguoro, Dipartimento di Informatica, Università di Torino, c.so Svizzera 185, 10149 Torino, Italy. Phone +39 011 6706711 - fax +39 011 751603. E-mail address: {stefano,deligu}@di.unito.it
Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies show this notice on the first page or initial screen of a display along with the full citation. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, to redistribute to lists, or to use any component of this work in other works requires prior specific permission and/or a fee. Permissions may be requested from Publications Dept., ACM, Inc., 2 Penn Plaza, Suite 701, New York, NY 10121-0701 USA, fax +1 (212) 869-0481, or permissions@acm.org.
© 201? ACM 1539-9087/201?/-ART00 $10.00
DOI 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

On the other hand consider the functional:

$$F(f,g,h,x) = \textbf{if } f(x) > f(g(x)) \textbf{ then } F(f,g,h,g(x)) \\ \textbf{else if } f(x) > f(h(x)) \textbf{ then } F(f,g,h,h(x)) \textbf{ else } x$$

It is a total recursive functional: otherwise there would be an infinite descending sequence $f(n_0) > f(n_1) > \cdots$ where $n_0, n_1, \ldots$ are the values of x in the recursive calls of F[1]. Clearly $F(f,g,h,n_0)$ computes a solution of the problem $f(x) \leq f(g(x)) \wedge f(x) \leq f(h(x))$, for any $n_0 \in \mathbb{N}$.

The functional F "learns" about the minimum of $\mathrm{rng}(f)$ from the counterexamples $f(x) > f(g(x))$ and $f(x) > f(h(x))$, by modifying its guess about the proper value of x, so effectively approximating the uncomputable minimum of $\mathrm{rng}(f)$. What is implicit in this construction is the fact that any computation of F can be resumed, and from any point in $\mathbb{N}$, to get a better approximation of the minimum of f that could be required in case of using (1) in some larger proof. Further there is an internal "dialogue" between the search attempting to satisfy $f(x) \leq f(g(x))$ and that to satisfy $f(x) \leq f(h(x))$, which is ruled by the particular protocol described in the definition of F: first attempt to satisfy $f(x) \leq f(g(x))$, then try to satisfy $f(x) \leq f(h(x))$, and repeat in this order until both goals are satisfied. However the two searches correspond to two distinct parts of the proof; so they should be treated independently, and even computed in parallel. Therefore in the paper we will factor out the internal protocol of interaction between them.

The shift from direct computation to search and learning can be understood as a change in the denotation of terms and formulas. In the perspective proposed in this paper the interpretation of a (closed) term t is not a number in $\mathbb{N}$, but a function α in $\mathbb{N}^{\mathbb{S}}$, where $\mathbb{S}$ is a partially ordered set of "states of knowledge". The value $\alpha(s)$ represents the guess about the value of t at state s. For this to make sense we require that α is eventually constant along any ω-chain of states $s_0 \sqsubseteq s_1 \sqsubseteq \cdots$: we call such an α an "individual". As a consequence also the meaning of a formula A, which in turn depends on the denotations of the terms occurring in A, is an individual, this time in $\mathbb{B}^{\mathbb{S}}$ where $\mathbb{B}$ is the set of booleans. As foretold, we interpret proofs into realizers. These are the core part of strategies such that, given an individual α and an arbitrary initial state s_0 we can build a sequence out of s_0 always reaching some larger $s' \sqsupseteq s_0$ effectively and within a finite number of steps, such that if $A(t)$ is the conclusion of the proof then $A(\alpha(s'))$ is true in the standard model of arithmetic.

We work out the construction in the quantifier free theory $\mathbf{PRA} + \mathbf{EM}_1$, which is essentially primitive recursive arithmetic plus $\mathbf{EM}_1$, that is excluded middle restricted to Σ^0_1 formulas. To avoid technical difficulties due to the treatment of quantifiers, we express $\mathbf{EM}_1$ by means of choice functions, which are not computable in general, though they are recursive in the limit.

Individuals are preserved by functions of a certain kind: we call them "convergent global" because of the restricted use of the state parameter. Individuals and convergent global functions form a category $\mathcal{G}$, which turns out to be cartesian, and so it is suitable to interpret the language of the theory $\mathbf{PRA} + \mathbf{EM}_1$, which is a (multisorted) algebraic theory.

The interpretation of terms and formulas in $\mathcal{G}$ is one of the two pillars of our construction. The second and most relevant one is the concept of "interactive realizer". Realizers are individuals in $\mathbb{S}^{\mathbb{S}}$ satisfying certain further conditions, implying that the prefixed points of any realizer, which we abstractly see as the goal of the learning agent, are cofinal in $\mathbb{S}$. Then we define the notion of "interactive forcing" as a relation between a realizer, a tuple of individuals over $\mathbb{N}$ and a formula, and prove that if a formula $A(t)$ is a theorem of $\mathbf{PRA} + \mathbf{EM}_1$ then there exists a realizer that, by interacting with the state, forces any individual in $\mathbb{N}^{\mathbb{S}}$ interpreting t to satisfy the formula $A(x)$.

Realizers are total recursive functionals. The construction of the realizer forcing a formula follows the proof of the formula itself. Realizers interpreting subproofs are combined by a binary operation which we call "merge". The merge operation is a parameter of our construction, expressing the internal protocol of interaction between subproofs. It is axiomatically defined, without committing to particular and somewhat arbitrary definitions, and obtaining at the same time a compositional interpretation of proofs. Moreover those parts of the proof which do not have computational meaning are automatically interpreted into a trivial realizer, that is the unit of the merge; therefore the realizer obtained in this way is a representation of the computational content of the given proof.

[1]This is a semiconstructive argument, but the totality of F can be constructively established by well founded induction.

1.1. Related Work

The idea of interactive realizability appeared first in [Berardi 2005] and developed in [Berardi and de'Liguoro 2008], together with the theory $\mathbf{PRA} + \mathbf{EM}_1$. The original construction was quite involved, due to the fact that a realizer was deemed to compute directly its least fixed point above a given state. In [Aschieri and Berardi 2010] and [Aschieri 2011] interactive realizers have been extended to $\mathbf{HA} + \mathbf{EM}_1$, by combining them with Kleene's realizability. As a matter of fact one could see Kleene realizability as a degenerate case of interactive realizability, where all realizers of atomic formulas never access the state and are constantly equal to the empty state. In the same works realizers of atomic formulas are regarded as adding to the state the missing facts, though moving to the meta-level the recursive definition of the chain reaching a (pre) fixed point of the realizer, a view that we adopt in the present paper. However the construction in [Aschieri and Berardi 2010] is syntactical in nature, leaving implicit much of the mathematical properties of the realizers and of the interpretation of formulas. On the other hand we are confident that the formulation in terms of individuals can be extended to $\mathbf{HA} + \mathbf{EM}_1$, where a realizer is not an "individual" in general. This non trivial task is left for further work.

The origins of the present work are in Coquand's "semantics of evidence" proposed in [Coquand 1995]. Under the influence of Gold's ideas in [Gold 1965; 1967] and of Hayashi's Limit Computable Mathematics (see e.g. [Hayashi 2006]) we have rephrased the dialogic interpretation of classical arithmetic by Coquand into a general theory of "learning" and "well founded limits" in [Berardi and de' Liguoro 2009], where the logical complexity of the goal is reflected by a ranking of the corresponding limit. We claim that interactive realizability is an instance of limit construction of rank 1, which is 1-backtracking in terms of [Berardi et al. 2005]. A study relating interactive realizability to 1-backtracking is [Aschieri 2010].

2. PROGRAM EXTRACTION IN THE THEORY $\mathbf{PRA} + \mathbf{EM}_1$

The theory of primitive recursive arithmetic, called **PRA** in [Troelstra and van Dalen 1988] (see vol. 1, chapter 3, section 2), is essentially the quantifier free fragment of Heyting arithmetic with equality. The language $\mathcal{L}_0$ of **PRA** is a first order algebraic language with two sorts or ground types Nat and Bool. It contains variables of type Nat[2], the constants $\mathsf{0}$ of type Nat and succ of type $\mathsf{Nat} \to \mathsf{Nat}$ for zero and successor respectively; further it includes a function symbol $\mathsf{f}, \mathsf{g}, \ldots$ of suitable types $\mathsf{Nat}^k \to \mathsf{Nat}$ for each primitive recursive function, the symbol $=$ of type $\mathsf{Nat}, \mathsf{Nat} \to \mathsf{Bool}$ for equality and the connectives $\neg, \wedge, \vee$ and $\to$ seen as operators of type $\mathsf{Bool} \to \mathsf{Bool}$ and $\mathsf{Bool}, \mathsf{Bool} \to \mathsf{Bool}$ respectively. To this list we add symbols for primitive recursive predicates $\mathsf{P}, \mathsf{Q}, \ldots$ of types $\mathsf{Nat}^k \to \mathsf{Bool}$ for the proper k, each with a fixed arity.

For presenting **PRA** we consider the following deductive system: the logical axioms are those of **IPC**, the intuitionistic propositional calculus, plus the axioms for equality; the non logical axioms include the defining equations of all primitive recursive functions and $\neg\, \mathsf{succ}(\mathsf{0}) = \mathsf{0}$. As explained in [Troelstra and van Dalen 1988], the formula $\mathsf{succ}(x) = \mathsf{succ}(y) \to x = y$ is derivable, and needs not to be assumed as an axiom. Inference rules are:

$$\frac{A \to B \quad A}{B}\,\mathrm{MP} \qquad \frac{A(x)}{A(t)}\,\mathrm{SUB} \qquad \frac{A(0) \quad A(x) \to A(\mathsf{succ}(x))}{A(y)}\,\mathrm{IND}$$

where in rule SUB the premise $A(x)$ has been derived from hypotheses not containing x.

By $A(x)$ we mean that x possibly occurs in A, and $A(t)$ denotes the same as the more explicit writing $A[t/x]$, namely the substitution of t for x in A. Although there are no bound variables in the formulas of $\mathcal{L}_0$, we speak of the sets $\mathrm{FV}(t)$ and $\mathrm{FV}(A)$ of the free variables occurring in t and A respectively.

Let us call $\mathbf{EM}_1$ the following schema, with $A \in \mathcal{L}_0$ such that $\mathrm{FV}(A) \subseteq \vec{x}, y$:

$$(\mathbf{EM}_1) \qquad \forall \vec{x}.\ \exists y\ A(\vec{x}, y) \vee \forall y\, \neg A(\vec{x}, y).$$

[2]Variables of type Bool are are propositional letters, and they are considered only in the proof of Lemma 5.6.

$\mathbf{EM}_1$ is just an instance of the law of excluded middle where $\exists y\, A(\vec{x}, y)$ is a Σ^0_1 formula with parameters, and it is called the Σ^0_1-**LEM** principle in the hierarchy studied by Akama et alii in [Akama et al. 2004]. $\mathbf{EM}_1$ uses nested quantifiers, hence it is not expressible by a formula in $\mathcal{L}_0$. To find a quantifier free equivalent of $\mathbf{EM}_1$ let us consider its classically equivalent prenex and skolemized normal form:

$$\forall \vec{x}, y.\ A(\vec{x}, \varphi(\vec{x})) \vee \neg A(\vec{x}, y),$$

which in turn is equivalent to

$$\forall \vec{x}, y.\ A(\vec{x}, y) \to A(\vec{x}, \varphi(\vec{x})). \tag{2}$$

Definition 2.1 (*The theory* $\mathbf{PRA} + \mathbf{EM}_1$). Let $\mathcal{L}_1$ be the language obtained by adding to $\mathcal{L}_0$ a functional symbol φ_{P} and a predicate symbol χ_{P} of arity k for each $k+1$-ary predicate symbol P of $\mathcal{L}_0$. The theory $\mathbf{PRA} + \mathbf{EM}_1$ is obtained by adding to the axioms of **PRA** the following axiom schemata:

$$(\chi)\ \ \mathsf{P}(\vec{x}, y) \to \chi_{\mathsf{P}}(\vec{x})$$
$$(\varphi)\ \ \chi_{\mathsf{P}}(\vec{x}) \to \mathsf{P}(\vec{x}, \varphi_{\mathsf{P}}(\vec{x}))$$

We do not add to $\mathcal{L}_0$ symbols for all Skolem functions for Peano arithmetic: only those relative to primitive recursive functions are considered. Since any formula of $\mathcal{L}_0$ defines a primitive recursive predicate, axioms (χ) and (φ) imply (2) and $\mathbf{EM}_1$, and in fact define a conservative extension of both theories. The actual meaning of $\chi_{\mathsf{P}}(\vec{x})$ is the predicate $\exists y.\ \mathsf{P}(\vec{x}, y)$. Concerning the interpretation of φ_{P}, a choice function for P, we note that the derivable implication $\mathsf{P}(\vec{x}, y) \to \mathsf{P}(\vec{x}, \varphi_{\mathsf{P}}(\vec{x}))$ is an instance of the *critical axiom* of Hilbert's ε-calculus [Hilbert and Bernays 1970], writing $\varphi_{\mathsf{P}}(\vec{x})$ in place of $\varepsilon y \mathsf{P}(\vec{x}, y)$, with the restriction that P has to be primitive recursive.

The restriction to primitive recursive predicates P in the language and axioms of $\mathbf{PRA} + \mathbf{EM}_1$ is responsible of the limitation to excluded middle of level 1, or equivalently of the fact that the implicit quantifications provided by the symbols χ_{P} and φ_{P} are not nested. This would be the case instead if we could use some φ_{Q} in the definition of the predicate P in χ_{P} or φ_{P}.

Let $\mathcal{T}$ be an arithmetical theory, possibly quantifier free to encompass the case of $\mathbf{PRA}+\mathbf{EM}_1$. We say that the *program extraction problem* in $\mathcal{T}$ has a solution if whenever $\mathcal{T} \vdash A(\vec{x}, t(\vec{x}))$ there exists an effective procedure associating to a proof of $A(\vec{x}, t(\vec{x}))$ in $\mathcal{T}$ a recursive function p computing t, that is for all $\vec{m} \in \mathbb{N}$, $p(\vec{m}) = t(\vec{m})$ is the number denoted by t when $\vec{m}$ is assigned to $\vec{x}$ in some specified interpretation of $\mathcal{T}$. With respect to the language $\mathcal{L}_1$ the intepretation of the new symbols χ_{P} and φ_{P} in $\mathcal{T}$ is the central task to construct p.

Now it is an elementary fact of logic that neither (the meaning of) χ_{P} nor φ_{P} are computable in general. More precisely, let $\mathcal{I}_0$ be the standard interpretation of $\mathcal{L}_0$ in **Set**, fixing $[\![\mathsf{Nat}]\!]^{\mathcal{I}_0} = \mathbb{N}$ as the set of numbers, and $[\![\mathsf{Bool}]\!]^{\mathcal{I}_0} = \mathbb{B} = \{\mathsf{true}, \mathsf{false}\}$ as that of booleans, and interpreting functional and predicate symbols by their recursion theoretic counterparts. Then $\mathcal{I}_0$ is a model of **PRA**, which we refer to as the *standard model*. On the other hand, since $\mathbf{PRA} + \mathbf{EM}_1$ is a subtheory of classical arithmetic with Skolem maps, there exist infinitely many interpretations $\mathcal{I}$ of $\mathcal{L}_1$ which extend $\mathcal{I}_0$ and are models of $\mathbf{PRA} + \mathbf{EM}_1$, though for some terms t and formulas A of $\mathcal{L}_1$, $[\![t]\!]^{\mathcal{I}}$ and $[\![A]\!]^{\mathcal{I}}$ are not recursive in any model $\mathcal{I}$ of $\mathbf{PRA} + \mathbf{EM}_1$. It follows that the program extraction problem in $\mathbf{PRA} + \mathbf{EM}_1$ is unsolvable w.r.t. any model. On the contrary we claim that if $A(\vec{x}, t(\vec{x}))$ is a theorem of $\mathbf{PRA} + \mathbf{EM}_1$, then there exists a recursive function $p(\vec{x})$ such that:

$$\forall \vec{m} \in \mathbb{N}\ \exists \mathcal{I} \supseteq \mathcal{I}_0.\ [\![A(\vec{m}, t(\vec{m}))]\!]^{\mathcal{I}} = \mathsf{true}\ \ \&\ \ p(\vec{m}) = [\![t(\vec{m})]\!]^{\mathcal{I}}, \tag{3}$$

where $\mathcal{I} \supseteq \mathcal{I}_0$ is informal for $\mathcal{I}$ is an extension of $\mathcal{I}_0$ to $\mathcal{L}_1$. Note that $\mathcal{I}$ is just an interpretation of $\mathcal{L}_1$ and that it is not required that $\mathcal{I} \models \mathbf{PRA} + \mathbf{EM}_1$.

In (3) the interpretation $\mathcal{I}$ is implicitly computed by p depending on $\vec{m}$. More precisely the computation of $p(\vec{m})$ consists of the construction of an approximation of a model of the whole theory $\mathbf{PRA}+\mathbf{EM}_1$ accurate enough to validate (an instance of) A, a concept that we have to make precise.

Definition 2.2 (*Consistency, Facts and States of Knowledge*). Let $\mathsf{P}(\vec{m}, n), \mathsf{Q}(\vec{m}', n'), \ldots$ be closed atomic formulas of $\mathcal{L}_0$, with $\mathsf{P}, \mathsf{Q}, \ldots$ symbols of primitive recursive predicates:

(1) $\mathsf{P}(\vec{m},n)$ and $\mathsf{Q}(\vec{m}',n')$ are *consistent* if $\mathsf{P}\equiv\mathsf{Q}$ and $\vec{m}=\vec{m}'$ implies $n=n'$, where $\equiv$ is syntactical identity;
(2) $\mathsf{P}(\vec{m},n)$ is a *fact* if $[\![\mathsf{P}(\vec{m},n)]\!]^{\mathcal{I}_0}=\mathsf{true}$;
(3) a *state of knowledge* (shortly a *state*) is a finite set of pairwise consistent facts: we call $\mathbb{S}$ the set of states of knowledge.

States of knowledge can be presented as a structure $(\mathbb{S},\sqsubseteq,\bot,\sqcup)$, where $(\mathbb{S},\sqsubseteq)$ is the partial order defined by $s\sqsubseteq s'$ if and only if $s\subseteq s'$; $\mathbb{S}$ has a bottom element $\bot=\emptyset$ and join of compatible states, $s\sqcup s'=s\ \cup\ s'$, where s,s' are *compatible*, written $s\uparrow s'$, if $s,s'\sqsubseteq s''$ for some $s''\in\mathbb{S}$. $\mathbb{S}$ is also downward closed, so that it is closed under (arbitrary non-empty) intersections.

From the fact that $\mathsf{P}\equiv\mathsf{Q}$ is syntactical identity it follows that membership to $\mathbb{S}$ is decidable. By the finiteness of the states $s\in\mathbb{S}$, the order and the compatibility relations are computable, as well as the join of two compatible states.

A state of knowledge $s=\{\mathsf{P}_1(\vec{m}_1,n_1),\dots,\mathsf{P}_k(\vec{m}_k,n_k)\}$ is a finite piece of information about the standard model $\mathcal{I}_0$ of **PRA**: it says for which tuples of natural numbers the predicates $[\![\mathsf{P}_i]\!]^{\mathcal{I}_0}$ are known to be true. The consistency condition implies that in each state of knowledge s there exists at most one witness n of the existential statement $\exists y.\mathsf{P}(\vec{m},y)$, namely of $\chi_{\mathsf{P}}(\vec{m})$, for each predicate P and tuple of natural numbers $\vec{m}$. This n is taken below as the value of $\varphi_{\mathsf{P}}(\vec{m})$ in the state s.

Definition 2.3. For each predicate symbol P of arity $k+1$, $\vec{m}=m_1,\dots,m_k\in\mathbb{N}$ and any (possibly infinite) consistent set of facts S, let:

$$[\![\chi_{\mathsf{P}}]\!](\vec{m},S)=\begin{cases}\mathsf{true} & \text{if } \mathsf{P}(\vec{m},n)\in S \text{ for some } n,\\ \mathsf{false} & \text{otherwise.}\end{cases}$$

Similarly define:

$$[\![\varphi_{\mathsf{P}}]\!](\vec{m},S)=\begin{cases}n & \text{if } \mathsf{P}(\vec{m},n)\in S \text{ for some } n,\\ 0 & \text{otherwise.}\end{cases}$$

Because of the consistency condition the value of $[\![\varphi_{\mathsf{P}}]\!](\vec{m},S)$ is unique. However there exist consistent sets of facts S such that $[\![\varphi_{\mathsf{P}}]\!](\vec{m},S)\neq[\![\varphi_{\mathsf{Q}}]\!](\vec{m},S)$ even if P and Q are equivalent as predicates, though they are different symbols. In this case either S includes some fact of P but not of Q, or $[\![\mathsf{P}]\!]^{\mathcal{I}_0}=[\![\mathsf{Q}]\!]^{\mathcal{I}_0}$ is a non functional predicate. This is no contradiction: φ_{P} and φ_{Q} are also different symbols, and they might well denote different choice functions.

In case of a finite $s\in\mathbb{S}$, both $[\![\chi_{\mathsf{P}}]\!](\vec{m},s)$ and $[\![\varphi_{\mathsf{P}}]\!](\vec{m},s)$ are computable, while for a generic consistent set of facts S they are not. Note that the decidability of $[\![\chi_{\mathsf{P}}]\!](\vec{m},s)$ makes the default value 0 of $[\![\varphi_{\mathsf{P}}]\!](\vec{m},s)$ effectively distinguishable from its possible proper value 0, according to the fact that $\mathsf{P}(\vec{m},0)\in s$ or not. In any case $[\![\varphi_{\mathsf{P}}]\!]$ is a total function.

Any consistent set of facts S determines an interpretation $\mathcal{I}_S$ of $\mathcal{L}_1$ via Definition 2.3; in fact, while $\mathcal{I}_S$ coincides with $\mathcal{I}_0$ for the symbols in $\mathcal{L}_0$, for the extra symbols χ_{P} and φ_{P} of $\mathcal{L}_1$ we set:

$$[\![\chi_{\mathsf{P}}(\vec{m})]\!]^{\mathcal{I}_S}=[\![\chi_{\mathsf{P}}]\!](\vec{m},S)\quad\text{and}\quad[\![\varphi_{\mathsf{P}}(\vec{m})]\!]^{\mathcal{I}_S}=[\![\varphi_{\mathsf{P}}]\!](\vec{m},S).$$

We are now in place to explain in which sense a state s is a finite approximation of model $\mathcal{I}$ of $\mathbf{PRA}+\mathbf{EM}_1$.

PROPOSITION 2.4. *Let S be an arbitrary set of facts. Then S determines a model $\mathcal{I}_S$ of* $\mathbf{PRA}+\mathbf{EM}_1$ *if and only it is consistent and maximal w.r.t. inclusion. Vice versa any model $\mathcal{I}$ of* $\mathbf{PRA}+\mathbf{EM}_1$ *extending the interpretation $\mathcal{I}_0$ determines a maximal consistent set of facts $S_{\mathcal{I}}$, and the constructions $\mathcal{I}_S$ and $S_{\mathcal{I}}$ are inverse each other.*

Moreover for any model $\mathcal{I}$ and expression $E\in\mathcal{L}_1$ (either a term or a formula) $[\![E]\!]^{\mathcal{I}}$ depends on a finite $s\subseteq S_{\mathcal{I}}$ only.

Proof. It is straightforward to see that $\mathcal{I}_S$ models both (χ) and (φ) axioms. In particular, if $[\![\mathsf{P}(\vec{m},n)]\!]^{\mathcal{I}_S}=[\![\mathsf{P}(\vec{m},n)]\!]^{\mathcal{I}_0}=\mathsf{true}$ then $\mathsf{P}(\vec{m},n)$ is a fact. Because of the maximality of S there exists n' such that $\mathsf{P}(\vec{m},n')\in S$, so that $[\![\chi_{\mathsf{P}}(\vec{m})]\!]^{\mathcal{I}_S}=\mathsf{true}$.

Vice versa let $\mathcal{I}$ be a model of $\mathbf{PRA}+\mathbf{EM}_1$, then

$$S_{\mathcal{I}} = \{\mathsf{P}(\vec{m},n) \mid [\![\mathsf{P}(\vec{m},n)]\!]^{\mathcal{I}} = \mathsf{true} \wedge [\![\varphi_{\mathsf{P}}(\vec{m})]\!]^{\mathcal{I}} = n\}$$

is a maximal consistent set of facts. Clearly $\mathcal{I}_{S_{\mathcal{I}}} = \mathcal{I}$ and $S_{\mathcal{I}_S} = S$.

That the interpretation $[\![E]\!]^{\mathcal{I}}$ depends on a finite $s \subseteq S_{\mathcal{I}}$ (a state) is easily established by structural induction, by observing in the base case that e.g. if $E = \chi_{\mathsf{P}}(\vec{m})$ for some P and $\vec{m}$, then either $[\![\chi_{\mathsf{P}}(\vec{m})]\!]^{\mathcal{I}} = \mathsf{true}$ so that we take $s = \{\mathsf{P}(\vec{m}, [\![\varphi_{\mathsf{P}}(\vec{m})]\!]^{\mathcal{I}})\}$, or $[\![\chi_{\mathsf{P}}(\vec{m})]\!]^{\mathcal{I}} = \mathsf{false}$, hence $s = \bot = \emptyset$. ■

By this proposition any model of $\mathbf{PRA}+\mathbf{EM}_1$ extending $\mathcal{I}_0$ can be obtained as the union of an ω-chain in $\mathbb{S}$ and the interpretation maps $[\![\cdot]\!]^{\mathcal{I}}$ are Scott continuous (w.r.t. the canonical Scott topology over the maximal consistent sets $S_{\mathcal{I}}$), and indeed computable. So a way to effectively approximate a model $\mathcal{I}$ of $\mathbf{PRA}+\mathbf{EM}_1$ is to devise a procedure generating a chain $s_0 \sqsubseteq s_1 \sqsubseteq \cdots$ in $\mathbb{S}$ such that $S_{\mathcal{I}} = \bigcup_i s_i$.

Because of the continuity of the interpretation maps, we know that to compute the value of an expression of $\mathcal{L}_1$ it suffices a finite initial segment of a chain of states. This implies that, given a theorem $A(\vec{x}, t(\vec{x}))$ of $\mathbf{PRA}+\mathbf{EM}_1$ and values $\vec{m}$ for the variables $\vec{x}$, we can effectively find a state s such that $A(\vec{m}, t(\vec{m}))$ is true in s. The finite state s is sufficient to evaluate the term $t(\vec{m})$ in $\mathcal{I}_S$, solving the problem (3).

As a final remark we observe that, as in the case of (1) in the Introduction, once we know that $\mathbf{PRA}+\mathbf{EM}_1 \vdash A$, a brute force search of some s making A true trivially exists: since facts are recursively enumerable, it suffices to ensure that the relevant facts, if any, are eventually added to the state.

However the result we obtain in Section 5 is much stronger, because we obtain a constructive interpretation of proofs in $\mathbf{PRA}+\mathbf{EM}_1$, which cannot be achieved by means of the trivial search algorithm.

3. THE CATEGORY OF INDIVIDUALS AND CONVERGENT GLOBAL FUNCTIONS

In this section we treat the mathematical structure in which we interpret both terms and formulas of $\mathcal{L}_1$ as well as the proofs of $\mathbf{PRA}+\mathbf{EM}_1$. We introduce the concepts of individuals and of functions preserving them, which we call global and convergent functions. An individual on X is a mapping from $\mathbb{S}$ to X satisfying a convergence property along any ω-chain of states.

In the following we work with subcategories of **Set**. We use the simply typed λ-calculus as a metanotation for functions, and types for sets. Because of the well known isomorphism $X \times Y \to Z \simeq X \to (Y \to Z)$, the same function will be written both in the uncurried form: $f(x,y)$ and in the curried one: $f\,x\,y$, according to convenience; also the more familiar notation $f(x)$ is preferred to $f\,x$. We write $\lambda\_ : Z\,.x$, or simply $\lambda\_\,.x$ when Z is understood, to denote the function from Z to X constantly equal to x.

Definition 3.1 (*Individuals and Convergent Global Functions*). Let X be any set; we say that a map $u : \mathbb{N} \to X$ has a *limit point* $x = \lim_i u(i) \in X$ if

$$\exists i\, \forall j.\ u(i) = u(i+j) = x.$$

A map $\sigma : \mathbb{N} \to \mathbb{S}$ is an *ω-chain* over $\mathbb{S}$ if $\sigma(i) \sqsubseteq \sigma(j)$ for all $i \leq j$. A map $\alpha \in X^{\mathbb{S}}$ is an *individual of* X if $\alpha \circ \sigma : \mathbb{N} \to X$ has a limit point for all ω-chain σ. We denote by $I(X)$ the set of individuals of X.

A function $g : X^{\mathbb{S}} \to Y^{\mathbb{S}}$ *has a global state*, shortly it is *global*, if

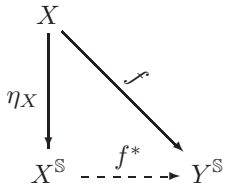
$$g(\alpha, s) = g(\lambda\_ : \mathbb{S}\,.\alpha(s), s),$$

for all $\alpha \in X^{\mathbb{S}}$ and $s \in \mathbb{S}$. A global g is *convergent* if $g(\lambda\_ : \mathbb{S}\,.x)$ is an individual for all $x \in X$.

Global functions can evaluate their functional argument α in the second argument s only: that is they have essentially a unique global state, whence the name. In fact a non global $f : X^{\mathbb{S}} \to Y^{\mathbb{S}}$ is easily constructed by violating this constrain: let $\alpha \in X^{\mathbb{S}}$ and $h : \mathbb{S} \to \mathbb{S}$ be such that $h(s) = s'$ and $\alpha(s) \neq \alpha(s')$ for certain $s, s' \in \mathbb{S}$; then the function $f := \lambda\beta\,.\beta \circ h$ is not global since $f(\alpha, s) = \alpha(h(s)) = \alpha(s')$, while $f(\lambda\_\,.\alpha(s), s) = (\lambda\_\,.\alpha(s))(h(s)) = \alpha(s)$.

A global function is determined by its values over constant individuals $\lambda\_.x$. In fact there exists an extension mapping $\_^*$ associating uniquely a convergent global function $f^* : X^{\mathbb{S}} \to Y^{\mathbb{S}}$ to any function $f : X \to Y^{\mathbb{S}}$ such that $f(X) \subseteq I(Y)$.

PROPOSITION 3.2. *Let $f : X \to Y^{\mathbb{S}}$ be such that $f(x) \in I(Y)$ for all $x \in X$. Then there exists a unique convergent global $f^* : X^{\mathbb{S}} \to Y^{\mathbb{S}}$ such that the following diagram commutes:*



where $\eta_X(x) = \lambda\_.x$ for all $x \in X$. Moreover all the convergent global functions arise in this way.

PROOF. Define $f^*(\alpha, s) = f(\alpha(s), s)$ for $\alpha \in X^{\mathbb{S}}$ and $s \in \mathbb{S}$. Then

$$f^*(\alpha, s) = f(\alpha(s), s) = f((\lambda\_.\alpha(s))(s), s) = f^*(\lambda\_.\alpha(s), s)$$

so that f^* is global. Now

$$(f^* \circ \eta_X)(x, s) = f^*(\lambda\_.x, s) = f(x, s)$$

which implies that the diagram commutes and, at the same time, that f^* is convergent global by the hypothesis on f. On the other hand if $g \circ \eta_X = f$ for some (convergent) global g then, since $\lambda\_.\alpha(s) = \eta_X(\alpha(s))$, we have

$$g(\alpha, s) = g(\lambda\_.\alpha(s), s) = (g \circ \eta_X)(\alpha(s), s) = f(\alpha(s), s),$$

so that $g(\alpha, s) = f^*(\alpha, s)$.

Finally given any convergent global $g : X^{\mathbb{S}} \to Y^{\mathbb{S}}$ take $\hat{g} : X \to Y^{\mathbb{S}}$ defined by $g \circ \eta_X$, that is by $x \mapsto g(\lambda\_.x)$: then for all $x \in X$ it is the case that $\hat{g}(x) \in I(Y)$ by the hypothesis, and $g = \hat{g}^*$. □

From the proof above we get a characterization of the convergent global functions in terms of the $\_^*$ operation, together with its inverse $\hat{g}(x) = g(\lambda\_.x)$.

The actual content of the last proposition is that $(\mathcal{S}, \eta, \_^*)$ where:

$$\begin{array}{lcl} \mathcal{S}(X) & = & X^{\mathbb{S}} \\ \eta_X(x) & = & \lambda\_.x \\ f^*(\alpha, s) & = & f(\alpha(s), s) \end{array}$$

is a Kleisli triple over **Set**, hence a monad. It is in fact a strong monad in the sense of [Moggi 1991], with (unique) tensorial strength $t_{X,Y} : X \times \mathcal{S}Y \to \mathcal{S}(X \times Y)$ given by:

$$t_{X,Y}(x, \alpha) = \lambda s : \mathbb{S}.\ (x, \alpha(s))$$

It is a submonad of Moggi's side-effect monad $(X \times \mathbb{S})^{\mathbb{S}}$, also called "state monad" in the functional programming community. Indeed we might think of $\mathbb{S}$ as the space of stores $\mathit{Val}^{\mathit{Loc}}$ where $\mathit{Val} = \mathbb{N} \cup \mathbb{B}$ and $\mathit{Loc} = \{\varphi_{\mathsf{P}}(\vec{m}), \chi_{\mathsf{P}}(\vec{m}) \mid \mathsf{P} \in \mathcal{L}_0, \vec{m} \in \mathbb{N}\}$, so that $[\![\varphi_{\mathsf{P}}]\!](\vec{m}, s)$ and $[\![\chi_{\mathsf{P}}]\!](\vec{m}, s)$ are the values of the basic lookup primitives applied to the "store" s. No state update operation is provided by the monad $\mathcal{S}$: this shall be regarded in the next sections as an external action over individuals instead.

The next theorem establishes that a convergent global function sends individuals to individuals. Note that in the example before Proposition 3.2, if h is an individual (which makes sense as $h \in \mathbb{S}^{\mathbb{S}}$) then the non global f still sends individuals to individuals, so that the latter property is not sufficient for a function to be global.

THEOREM 3.3 (CONVERGENCE THEOREM). *If $g : X^{\mathbb{S}} \to Y^{\mathbb{S}}$ is global and convergent then $g(\alpha) \in I(Y)$ for all individuals $\alpha \in I(X)$.*

PROOF. Let $\alpha \in X^{\mathbb{S}}$ be an individual; then for any ω-chain of states σ there exists $i_0 \in \mathbb{N}$ such that for all $j \geq i_0$, $\alpha(\sigma(i_0)) = \alpha(\sigma(j))$. Since g is global, we know that $g(\alpha, s) = g(\lambda\_.\alpha(s), s)$ for all $s \in \mathbb{S}$; therefore

$$g(\alpha, \sigma(j)) = g(\lambda\_.\alpha(\sigma(j)), \sigma(j)) = g(\lambda\_.\alpha(\sigma(i_0)), \sigma(j)),$$

for all $j \geq i_0$. By the hypothesis that $g(\alpha)$ is an individual for all constant α it follows that $g(\lambda\_.\alpha(\sigma(i_0))) \in I(Y)$, so that there exists i_1 such that for all $k \geq i_1$,

$$g(\lambda\_.\alpha(\sigma(i_0)), \sigma(k)) = g(\lambda\_.\alpha(\sigma(i_0)), \sigma(i_1)).$$

Then for all $h \geq \max(i_0, i_1)$:

$$g(\alpha, \sigma(h)) = g(\lambda\_.\alpha(\sigma(i_0)), \sigma(h)) = g(\lambda\_.\alpha(\sigma(i_0)), \sigma(i_1)).$$

We conclude that $g(\alpha) \in I(Y)$. □

COROLLARY 3.4. *If $f : X^{\mathbb{S}} \to Y^{\mathbb{S}}$ and $g : Y^{\mathbb{S}} \to Z^{\mathbb{S}}$ are (convergent) global then $g \circ f$ is such.*

PROOF. For all $\alpha \in X^{\mathbb{S}}$ and $s \in \mathbb{S}$:

$$(g \circ f)(\alpha, s) = g(f(\alpha), s) = g(\lambda\_.f(\alpha, s), s) = g(\lambda\_.f(\lambda\_.\alpha(s), s), s).$$

On the other hand:

$$(g \circ f)(\lambda\_.\alpha(s), s) = g(f(\lambda\_.\alpha(s)), s) = g(\lambda\_.f(\lambda\_.\alpha(s), s), s),$$

hence $(g \circ f)(\alpha, s) = (g \circ f)((\lambda\_\alpha(s), s)$ and $g \circ f$ is a global function. Moreover, if both f and g are convergent, we have that $\beta = f(\lambda\_.x)$ is an individual, so that $(g \circ f)(\lambda\_.x) = g(\beta)$ is an individual by Theorem 3.3. We conclude that $g \circ f$ is convergent. □

Since $\mathtt{Id}_{X^{\mathbb{S}}} : X^{\mathbb{S}} \to X^{\mathbb{S}}$ with $\mathtt{Id}_{X^{\mathbb{S}}}(\alpha, s) = \alpha(s) = (\lambda\_.\alpha(s))(s)$ is global and trivially convergent, we have that the following is a category.

Definition 3.5 (*The Category of Individuals and Convergent Global Functions*). The *category of individuals and convergent global functions* $\mathcal{G}$ is defined by the following data:

(1) the objects of $\mathcal{G}$ are sets of individuals $U \subseteq I(X)$, for any set X;
(2) if $U \subseteq I(X)$ and $V \subseteq I(V)$, $g \in \mathcal{G}(U, V)$ if and only if $g : U \to V$ in **Set** and there exists a convergent global $g' : X^{\mathbb{S}} \to Y^{\mathbb{S}}$ such that $g = g' \restriction U$.

For $U \in |\mathcal{G}|$, $U \subseteq I(X)$ and $\alpha \in U$ define $\mathrm{rng}(\alpha) = \{\alpha(s) \mid s \in \mathbb{S}\} \subseteq X$ and $\mathrm{rng}(U) = \bigcup\{\mathrm{rng}(\alpha) \mid \alpha \in U\}$. Then $U \subseteq I(\mathrm{rng}(U))$, and this is strict inclusion in general: take a non empty set X and $U = \{\lambda\_.x \mid x \in X\}$, so that $\mathrm{rng}(U) = X$ and $U \subset I(X)$. The identity $\mathtt{Id}_U$ is the identity of U in **Set**, which can be considered as the restriction of the convergent global $\mathtt{Id}_{X^{\mathbb{S}}}$ to U, where $X = \mathrm{rng}(U)$. Composition in $\mathcal{G}$ is ordinary composition in **Set**. So $\mathcal{G}$ is a subcategory of **Set**.

As a matter of fact the set valued function I extends to a functor, which is a submonad of $(-)^{\mathbb{S}}$, in virtue of Proposition 3.2. However $\mathcal{G}$ is not the Kleisli category of I. This is due to the freedom in choosing subsets of any $I(X)$ as objects of $\mathcal{G}$ and to the fact that the topology over $X^{\mathbb{S}}$ considered in the definition of convergence is coarse. Indeed take $X = \{0, 1\}$, and $U = \{\lambda\_.0, \lambda\_.1\} \subseteq I(X)$; consider the map $f : X \to U$ defined by $x \mapsto \lambda\_.x$, and take $\alpha : \mathbb{S} \to X$ be such that $\alpha(\bot) = 0$ and $\alpha(s) = 1$ whenever $s \neq \bot$. Then $\alpha \in I(X)$, and for all $s \in \mathbb{S}$, $f(\alpha(s)) \in U$; but $f^*(\alpha, s) = f(\alpha(s), s) = \alpha(s)$ for all s, so that $f^*(\alpha) = \alpha \notin U$.

Given $g \in \mathcal{G}(U, V)$ we shall write $g' : \mathrm{rng}(U)^{\mathbb{S}} \to \mathrm{rng}(V)^{\mathbb{S}}$ to indicate some convergent global function s.t. $g = g' \restriction U$, which exists by definition, though it is not uniquely determined by g; indeed g' is unique if U includes all the constant individuals.

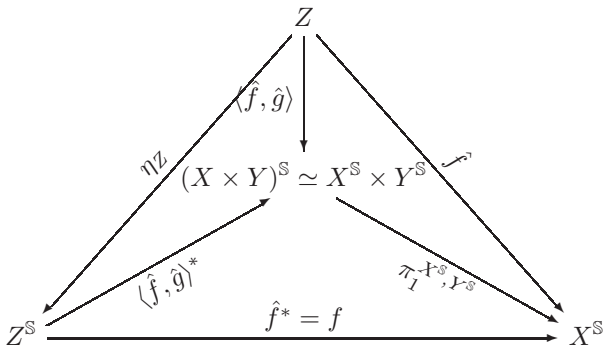
PROPOSITION 3.6. *$\mathcal{G}$ is cartesian. More precisely if $X = \mathrm{rng}(U)$ and $Y = \mathrm{rng}(V)$ then the product $U \times_{\mathcal{G}} V$ in $\mathcal{G}$ is given by $\{\langle \alpha, \beta \rangle \mid \alpha \in U, \beta \in V\} \subseteq I(X \times Y)$, with projections $\pi_i^{U,V} = \pi_i^{X,Y} \circ \_$, where $\pi_i^{X,Y}$ are the projections of $X \times Y$ in* **Set**. *For all $W \subseteq I(Z)$ and pair of morphisms $f \in \mathcal{G}(W, U)$ and*

$g \in \mathcal{G}(W,V)$ it turns out that $\langle f', g'\rangle = \langle \hat{f}', \hat{g}'\rangle^*$ where $f = f' \restriction W$ and $g = g' \restriction W$. It follows that the product morphism in $\mathcal{G}(W, U \times_{\mathcal{G}} V)$ is

$$\langle f, g\rangle_{\mathcal{G}} = \langle f', g'\rangle \restriction W.$$

PROOF. First observe that the functor $\mathcal{S} = (\_)^{\mathbb{S}}$, with arrow part $\mathcal{S}h = h \circ \_$, preserves all limits, so in particular it is a cartesian functor. Hence we have that $(X \times Y)^{\mathbb{S}} \simeq X^{\mathbb{S}} \times Y^{\mathbb{S}}$, $\mathcal{S}\pi_i^{X,Y} = \pi_i^{X^{\mathbb{S}},Y^{\mathbb{S}}} = \pi_i^{X,Y} \circ \_$ and if $h : Z \to X$ and $k : Z \to Y$ then $\mathcal{S}\langle h, k\rangle = \langle \mathcal{S}h, \mathcal{S}k\rangle$, where the last equalities are understood up to isomorphism of their domain and codomain respectively. Since $\mathcal{S}$ is also a monad with Kleisli extension $\_^*$, we have that e.g. $\mathcal{S}\pi_1^{X,Y} = (\eta_X \circ \pi_1^{X,Y})^*$, which by Proposition 3.2 implies that the $\mathcal{S}\pi_i^{X,Y}$ for $i = 1, 2$ are global functions. They are also convergent, because e.g. $(\pi_1^{X,Y} \circ \_)(\lambda\_.(x, y)) = \lambda\_.x$.

Finally let us identify $f' : Z^{\mathbb{S}} \to X^{\mathbb{S}}$ and $g' : Z^{\mathbb{S}} \to Y^{\mathbb{S}}$ with $f : W \to U$ and $g : W \to V$ respectively, and consider the diagram:



Then $\hat{f} = \pi_1^{X^{\mathbb{S}},Y^{\mathbb{S}}} \circ \langle \hat{f}, \hat{g}\rangle$ being $\langle \hat{f}, \hat{g}\rangle$ the product arrow in **Set**, $\langle \hat{f}, \hat{g}\rangle = \langle \hat{f}, \hat{g}\rangle^* \circ \eta_Z$ and $\hat{f} = \hat{f}^* \circ \eta_Z$ by Proposition 3.2. So that:

$$\hat{f} = \pi_1^{X^{\mathbb{S}},Y^{\mathbb{S}}} \circ \langle \hat{f}, \hat{g}\rangle = \pi_1^{X^{\mathbb{S}},Y^{\mathbb{S}}} \circ \langle \hat{f}, \hat{g}\rangle^* \circ \eta_Z$$

which, by 3.2 again, implies $f = \hat{f}^* = \pi_1^{X^{\mathbb{S}},Y^{\mathbb{S}}} \circ \langle \hat{f}, \hat{g}\rangle^*$. Similarly we have that $g = \hat{g}^* = \pi_2^{X^{\mathbb{S}},Y^{\mathbb{S}}} \circ \langle \hat{f}, \hat{g}\rangle^*$. We then conclude that $\langle \hat{f}, \hat{g}\rangle^* = \langle f, g\rangle$ since $\langle f, g\rangle$ is the unique arrow in **Set** such that $f = \pi_1^{X^{\mathbb{S}},Y^{\mathbb{S}}} \circ \langle f, g\rangle$ and $g = \pi_2^{X^{\mathbb{S}},Y^{\mathbb{S}}} \circ \langle f, g\rangle$. By this and Proposition 3.2 we also know that $\langle f, g\rangle$ (i.e. $\langle \hat{f}, \hat{g}\rangle^*$) is global. To see that $\langle f, g\rangle$ is convergent note that $\langle \lambda\_.x, \lambda\_.y\rangle = \lambda\_.(x, y)$. □

We end this section by extending the notion of convergent global function to k-ary functions.

Definition 3.7 (*Convergent k-Global Functions*). Let $f : X_1^{\mathbb{S}} \times \cdots \times X_k^{\mathbb{S}} \to Y^{\mathbb{S}}$, with $k \geq 1$, be a function; then f is *k-global* if and only if for all $\alpha_1 \in X_1^{\mathbb{S}}, \ldots, \alpha_k \in X_k^{\mathbb{S}}$ and $s \in \mathbb{S}$

$$f(\alpha_1, \ldots, \alpha_k, s) = f(\lambda\_.\alpha_1(s)), \ldots, \lambda\_.\alpha_k(s), s).$$

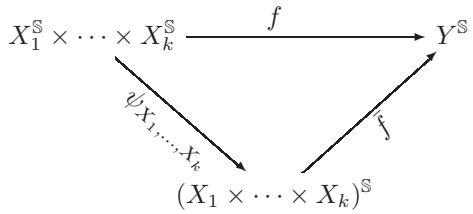
It is *convergent* if also $f(\lambda\_.x_1, \ldots, \lambda\_.x_k) \in I(Y)$ for all $x_1 \in X_1, \ldots, x_k \in X_k$.

Define

$$\begin{array}{rcl} \psi_{X_1,\ldots,X_k} : X_1^{\mathbb{S}} \times \cdots \times X_k^{\mathbb{S}} & \longrightarrow & (X_1 \times \cdots \times X_k)^{\mathbb{S}} \\ (\alpha_1, \ldots, \alpha_k) & \mapsto & \langle \alpha_1, \ldots, \alpha_k\rangle \end{array}$$

LEMMA 3.8. *For all $X_1, \ldots, X_k$, $\psi_{X_1,\ldots,X_k}$ is an iso with inverse $\gamma \mapsto (\pi_1 \circ \gamma, \ldots, \pi_k \circ \gamma)$, and it is such that for any $f : X_1^{\mathbb{S}} \times \cdots \times X_k^{\mathbb{S}} \to Y^{\mathbb{S}}$ there exists a unique $\bar{f} : (X_1 \times \cdots \times X_k)^{\mathbb{S}} \to Y^{\mathbb{S}}$ such that*

$f = \bar{f} \circ \psi_{X_1,\ldots,X_k}$ that is the following diagram commutes:



Moreover f is (convergent) k-global if and only if $\bar{f}$ is (convergent) global.

PROOF. That $\psi_{X_1,\ldots,X_k}$ is an iso follows by induction over k and the fact that $X^{\mathbb{S}} \times Y^{\mathbb{S}} \simeq (X \times Y)^{\mathbb{S}}$ are isomorphic via the map $(\alpha, \beta) \mapsto \langle \alpha, \beta \rangle$. Being an iso in **Set**, it sends k-tuples of constant functions into constant functions, which can be seen directly by observing that:

$$\psi_{X_1,\ldots,X_k}(\lambda\_.x_1, \ldots, \lambda\_.x_k) = \langle \lambda\_.x_1, \ldots, \lambda\_.x_k \rangle = \lambda\_.(x_1, \ldots, x_k).$$

The rest is obvious since $\bar{f}$ must be $f \circ \psi^{-1}_{X_1,\ldots,X_k}$. □

Notably the isomorphisms ψ are definable in terms of the tensorial strength t of $\mathcal{S}$, along the lines of Remark 3.6 in [Moggi 1991], from which we borrow the notation.

4. INTERACTIVE REALIZERS

This section introduces the central concept of *interactive realizer* which, together with the related notion of *interactive forcing* in the next section, are the main contribution of our work. Realizers have been introduced by Kleene as an interpretation of Brouwer's and Heyting's concept of construction. In the case of constructive theories a realizer is a direct computation, possibly depending on some parameters. With a non constructive theory like $\mathbf{PRA} + \mathbf{EM}_1$ the saving of such an idea involves the shift from recursiveness to recursiveness in the limit and learning in the sense of Gold. In this perspective a realizer is not an algorithm (a recursive function), rather it is the recursive generator of a search procedure that, along a series of attempts and failures, eventually attains its goal.

Formally, interactive realizers are certain maps over $\mathbb{S}$. They tell which facts have to be added to a state to reach their goals. The goals of a realizer are abstractly defined as the states to which the realizer does not add any fact, because the goal is attained.

Definition 4.1 (*Interactive Realizers*). An *interactive realizer* (shortly a *realizer*) is a map $r \in \mathbb{S}^{\mathbb{S}}$, such that:

(1) $r \in I(\mathbb{S})$;
(2) $r(s) \uparrow s$ for all $s \in \mathbb{S}$;
(3) $r(s) \cap s = \bot$ for all $s \in \mathbb{S}$.

We call $\mathbb{R}$ the set of realizers. A state $s \in \mathbb{S}$ is a *prefix point* of $r \in \mathbb{R}$ if $r(s) \sqsubseteq s$; we set $\mathit{Prefix}\,(r) = \{s \in \mathbb{S} \mid r(s) \sqsubseteq s\}$.

By clause (1) the realizers are particular individuals over $\mathbb{S}$. Note that identity over $\mathbb{S}$ is not convergent, and so it is not a realizer. Compatibility condition (2) is essential, together with convergence, for the existence of pre-fixed points (see below). The function $\lambda\_.\bot$ is a (trivial) realizer and, because of clause (3), the only one among constant individuals.

By clause (3), if r is a realizer then $s \in \mathit{Prefix}\,(r)$ if and only if $r(s) = \bot$, because $r(s) \sqsubseteq s$ implies $r(s) = r(s) \cap s = \bot$. This clause is just intended to simplify the treatment of realizers by making them irredundant in the sense that $r(s)$ just adds only "new" facts to s; hence $r(s) \sqsubseteq s$ means that there is actually nothing to add.

PROPOSITION 4.2 (COFINALITY OF REALIZERS PREFIX POINTS). *If $r \in \mathbb{R}$ then for all $s \in \mathbb{S}$ there is $s' \in \mathit{Prefix}\,(r)$ such that $s \sqsubseteq s'$, namely $\mathit{Prefix}\,(r)$ is cofinal in $\mathbb{S}$ (in particular it is non empty).*

PROOF. Given $s \in \mathbb{S}$ define the mapping $\sigma : \mathbb{N} \to \mathbb{S}$ by $\sigma(0) := s$ and $\sigma(i+1) := \sigma(i) \sqcup r(\sigma(i))$, which exists because of the compatibility of r with its argument. By construction σ is an ω-chain, hence by the convergence of r, $r \circ \sigma$ has a limit $\sigma(i_0)$ for some i_0, that is $r(\sigma(i_0)) = r(\sigma(i_0+1))$. Then

$$\sigma(i_0+1) = \sigma(i_0) \sqcup r(\sigma(i_0)) = \sigma(i_0) \sqcup r(\sigma(i_0+1)),$$

which implies $r(\sigma(i_0+1)) \sqsubseteq \sigma(i_0+1)$; clearly $s = \sigma(0) \sqsubseteq \sigma(i_0+1) \in \mathit{Prefix}\,(r)$. □

Realizers can be combined by lifting to $\mathbb{S}^{\mathbb{S}}$ a binary operation over $\mathbb{S}$ which we call merge.

Definition 4.3 (*Merge*). A *merge* is a mapping $\bullet : \mathbb{S} \times \mathbb{S} \to \mathbb{S}$ such that, for all $s_1, s_2 \in \mathbb{S}$:

(1) $(\mathbb{S}, \bullet, \bot)$ is a monoid;
(2) if $s_1 \bullet s_2 = \bot$ then $s_1 = \bot = s_2$;
(3) $s_1 \bullet s_2 \subseteq s_1 \cup s_2$.

The merge of two states aims to remedy the partiality of the join in $\mathbb{S}$. To this end $s_1 \bullet s_2$ is some consistent choice of facts in $s_1 \cup s_2$, a set which in general is not consistent. Any merge has $\bot$ as unit, because when $\bot$ is merged with any s a consistent choice is s itself. Associativity is a natural requirement, though commutativity would be too restrictive. Clause (2) says that $s_1 \bullet s_2$ always saves same facts from $s_1 \cup s_2$ a soon as $s_1 \cup s_2$ is non empty; it will be essential in the proof of Proposition 4.7.

LEMMA 4.4. *If $\bullet$ is a merge then for all $s, s_1, s_2 \in \mathbb{S}$:*

(1) if $s \uparrow s_1$ and $s \uparrow s_2$ then $s \uparrow (s_1 \bullet s_2)$;
(2) if $s \cap s_1 = s \cap s_2 = \bot$ then $s \cap (s_1 \bullet s_2) = \bot$.

PROOF. (1): $s \not\gamma (s_1 \bullet s_2)$ implies that there exists $a \in s_1 \bullet s_2$ such that $s \not\gamma \{a\}$. Since $s_1 \bullet s_2 \subseteq s_1 \cup s_2$, it is the case that $a \in s_i$ for either $i = 1$ or $i = 2$, contradicting $s \uparrow s_1$ and $s \uparrow s_2$.
(2): we observe that $s \cap (s_1 \bullet s_2) \subseteq s \cap (s_1 \cup s_2) = (s \cap s_1) \cup (s \cap s_2)$, hence if $(s \cap s_1) \cup (s \cap s_2) = \bot = \emptyset$ then $s \cap (s_1 \bullet s_2) = \bot$. □

Merge operations do exist. A very simple example consists in dropping one of the merged states.

PROPOSITION 4.5. *The following mapping is a merge:*

$$s_1 \bullet_0 s_2 = \begin{cases} s_1 & \textit{if } s_1 \neq \bot, \\ s_2 & \textit{otherwise.} \end{cases}$$

PROOF. It is immediate that $s_1 \bullet_0 s_2 \in \mathbb{S}$ for all $s_1, s_2 \in \mathbb{S}$.
For all $s \in \mathbb{S}$, $\bot \bullet_0 s = s$. If $s = \bot$ then $s \bullet_0 \bot = \bot = s$. On the other hand if $s \neq \bot$ then $s \bullet_0 \bot = s$: hence $\bot$ is the unit of $\bullet_0$.
Let $s_1 = \bot$, then

$$(s_1 \bullet_0 s_2) \bullet_0 s_3 = s_2 \bullet_0 s_3 = s_1 \bullet_0 (s_2 \bullet_0 s_3).$$

Else, if $s_1 \neq \bot$ then

$$(s_1 \bullet_0 s_2) \bullet_0 s_3 = s_1 \bullet_0 s_3 = s_1 = s_1 \bullet_0 (s_2 \bullet_0 s_3).$$

Therefore (1) of Definition 4.3 holds.
If $s_1 \neq \bot$ then $s_1 \bullet_0 s_2 = s_1 \neq \bot$; similarly if $s_1 = \bot$ and $s_2 \neq \bot$ then $s_1 \bullet_0 s_2 = s_2 \neq \bot$, so that condition (2) of Definition 4.3 follows by contraposition.
Finally $s_1 \bullet_0 s_2 = s_i$ for either $i = 1, 2$, hence (3) of Definition 4.3 is satisfied. □

Remark 4.6. The map $\bullet_0$ is essentially a selector of non $\bot$-states, with a bias toward its first argument: it considers the second argument just in case the first one is not informative at all. In particular it is not commutative, while it is clearly idempotent: $s \bullet_0 s = s$. It is a very simple, though crude example of merge. Beside it and its symmetric $s_1 \bullet_0' s_2 := s_2 \bullet_0 s_1$, there exist other examples of merge that one could consider. We mention two of them omitting proofs.

— A "parallel" non-commutative merge. Define $\tilde{s} = \{\mathsf{P}(\vec{m}, n) \mid \exists n'.\mathsf{P}(\vec{m}, n') \in s\}$, and set

$$s_1 \bullet_1 s_2 := s_1 \cup (s_2 \setminus \tilde{s}_1).$$

This merge saves all of the information in s_2 which is consistent with s_1, while in case of inconsistency, the elements of s_1 prevail: hence it is not commutative, and its symmetric is a different merge. This is the merge operation used in [Aschieri and Berardi 2010].

— A "parallel" commutative merge. For any $X \subseteq \bigcup \mathbb{S}$ define $\widehat{X} := \{\mathsf{P}(\vec{m}, n) \in X \mid \forall\, \mathsf{P}(\vec{m}, n') \in X . n \leq n'\}$. Then we set:

$$s_1 \bullet_2 s_2 := \widehat{s_1 \cup s_2}.$$

The effect of $\widehat{X}$ is, for all predicate P and vector of numbers $\vec{m}$, to select, among all possibly inconsistent facts $\mathsf{P}(\vec{m}, n_1), \mathsf{P}(\vec{m}, n_2), \ldots$ in X, the fact $\mathsf{P}(\vec{m}, n_i)$, where n_i is the minimum among $n_1, n_2, \ldots$. It follows that $\widehat{X}$ is always consistent and, if X is finite, it is an element of $\mathbb{S}$. Moreover $\widehat{X} \subseteq X$ and $\widehat{\widehat{X}} = \widehat{X}$, hence it is an interior operator. The remarkable property of $\bullet_2$ is commutativity. This merge appears in [Berardi 2005].

We observe that $\bullet_0$, $\bullet_1$ and $\bullet_2$ are all computable functions.

Fix a merge operation $\bullet$, and define $\bullet^{\mathcal{S}} := \mathcal{S}(\bullet) \circ \psi_{\mathbb{S},\mathbb{S}}$, so that for any $r, r' \in \mathbb{R}$ and $s \in \mathbb{S}$ we have:

$$(r \bullet^{\mathcal{S}} r')(s) = r(s) \bullet r'(s)$$

where $\psi_{\mathbb{S},\mathbb{S}}(r, r') = \langle r, r' \rangle$.

PROPOSITION 4.7. *For any pair of realizers $r, r' \in \mathbb{R}$, $r \bullet^{\mathcal{S}} r'$ is a realizer such that:*

$$\textit{Prefix}\,(r \bullet^{\mathcal{S}} r') = \textit{Prefix}\,(r) \cap \textit{Prefix}\,(r').$$

PROOF. By Proposition 3.2 and Lemma 3.7, $\bullet^{\mathcal{S}}$ is a binary convergent global function, so that $r \bullet^{\mathcal{S}} r' \in I(\mathbb{S})$. For any $s \in \mathbb{S}$ we know that $s \uparrow r(s)$ and $s \uparrow r'(s)$; now $(r \bullet^{\mathcal{S}} r')(s) = r(s) \bullet r'(s)$ for all $s \in \mathbb{S}$ and we conclude that $s \uparrow (r(s) \bullet r'(s))$ by (1) of Lemma 4.4.

By (3) of Definition 4.1, $r(s) \cap s = \bot = r'(s) \cap s$; by (2) of Lemma 4.4 this implies:

$$(r \bullet^{\mathcal{S}} r')(s) \cap s = (r(s) \bullet r'(s)) \cap s = \bot.$$

This concludes the proof that $r \bullet^{\mathcal{S}} r'$ is a realizer. This fact implies that $\textit{Prefix}\,(r \bullet^{\mathcal{S}} r') = \{s \in \mathbb{S} \mid r(s) \bullet r'(s) = \bot\}$: by (2) of Definition 4.3 we know that $r(s) \bullet r'(s) = \bot$ implies both $r(s) = \bot$ and $r'(s) = \bot$, namely that $\textit{Prefix}\,(r \bullet^{\mathcal{S}} r') \subseteq \textit{Prefix}\,(r) \cap \textit{Prefix}\,(r')$. Viceversa, if $s \in \textit{Prefix}\,(r) \cap \textit{Prefix}\,(r')$ then $r(s) = \bot = r'(s)$, so that, by $\bot \bullet \bot = \bot$, we have that $r(s) \bullet r'(s) = \bot$, that is $s \in \textit{Prefix}\,(r \bullet^{\mathcal{S}} r')$. □

COROLLARY 4.8. *The structure $(\mathbb{R}, \bullet^{\mathcal{S}}, \lambda\_.\bot)$ is a monoid in $\mathcal{G}$.*

PROOF. By Proposition 4.7, $(\mathbb{R}, \bullet^{\mathcal{S}}, \lambda\_.\bot)$ is a sub monoid of $(\mathbb{S}^{\mathbb{S}}, \bullet^{\mathcal{S}}, \lambda\_.\bot)$. It is a monoid in $\mathcal{G}$ since $\mathbb{R} \subseteq I(\mathbb{S})$ and $\bullet^{\mathcal{S}}$ is global and convergent. □

5. INTERACTIVE FORCING AND THE INTERACTIVE REALIZABILITY THEOREM

We define the interpretation of $\mathcal{L}_1$ in the category $\mathcal{G}$ following the standard pattern of multisorted algebras or of algebraic type theory in the terms of [Crole 1993] chapter 3, which suffices because of the lack of quantifiers. First set $[\![\mathsf{Nat}]\!]^{\mathcal{G}} = I(\mathbb{N}) \subseteq \mathbb{N}^{\mathbb{S}}$ and $[\![\mathsf{Bool}]\!]^{\mathcal{G}} = I(\mathbb{B}) \subseteq \mathbb{B}^{\mathbb{S}}$. Next we proceed by constructing an interpretation $[\![\cdot]\!]^{\mathbb{S}}$ into the larger category $\mathbf{Set}^*_{\mathcal{S}}$, which is isomorphic to the Kleisli category $\mathbf{Set}_{\mathcal{S}}$ having sets of the shape $\mathcal{S}(X) = X^{\mathbb{S}}$ as objects, and maps $f^* : X^{\mathbb{S}} \to Y^{\mathbb{S}}$ for $f : X \to Y^{\mathbb{S}}$ as arrows. Since $\mathcal{G}$ can be faithfully embedded into $\mathbf{Set}^*_{\mathcal{S}}$, we define the interpretation $[\![\cdot]\!]^{\mathcal{G}}$ of terms and formulas in $\mathcal{L}_1$ by restricting the respective interpretations in $\mathbf{Set}^*_{\mathcal{S}}$ to the individuals in $I(\mathbb{N})$ and $I(\mathbb{B})$.

Let $\psi_{\mathbb{N}^k} : (\mathbb{N}^{\mathbb{S}})^k \to (\mathbb{N}^k)^{\mathbb{S}}$ denote $\psi_{\mathbb{N},\ldots,\mathbb{N}}$ with k occurrences of $\mathbb{N}$ in the subscript of ψ. We begin with the symbols in $\mathcal{L}_0 \subseteq \mathcal{L}_1$. For a k-ary functional symbol $\mathsf{f} \in \mathcal{L}_0$, where $[\![\mathsf{f}]\!]^{\mathcal{I}_0} : \mathbb{N}^k \to \mathbb{N}$, we define:

$$[\![\mathsf{f}]\!]^{\mathbb{S}} : (\mathbb{N}^{\mathbb{S}})^k \to \mathbb{N}^{\mathbb{S}} \quad \text{by} \quad [\![\mathsf{f}]\!]^{\mathbb{S}} = \mathcal{S}([\![\mathsf{f}]\!]^{\mathcal{I}_0}) \circ \psi_{\mathbb{N}^k}.$$

In particular if $[\![\mathsf{n}]\!]^{\mathcal{I}_0} = n$, then thinking of n as a point $n : 1 \to \mathbb{N}$ in $\mathbf{Set}$, we have $[\![\mathsf{n}]\!]^{\mathbb{S}} = \mathcal{S}(n) = (\eta_{\mathbb{N}} \circ n)^* = \lambda\_.n : 1^{\mathbb{S}} \to \mathbb{N}^{\mathbb{S}}$, where $1^{\mathbb{S}} \simeq 1$ is terminal in $\mathcal{G}$.

Similarly if $\mathsf{Q} \in \mathcal{L}_0$ is a k-ary predicate symbol we set:

$$[\![\mathsf{Q}]\!]^{\mathbb{S}} : (\mathbb{N}^{\mathbb{S}})^k \to \mathbb{B}^{\mathbb{S}} \quad \text{where} \quad [\![\mathsf{Q}]\!]^{\mathbb{S}} = \mathcal{S}([\![\mathsf{Q}]\!]^{\mathcal{I}_0}) \circ \psi_{\mathbb{N}^k}.$$

Let $\varphi_{\mathsf{P}} \in \mathcal{L}_1$ be the k-ary functional symbol associated to the $k+1$-ary predicate symbol $\mathsf{P} \in \mathcal{L}_0$; we define:

$$[\![\varphi_{\mathsf{P}}]\!]^{\mathbb{S}} : (\mathbb{N}^{\mathbb{S}})^k \to \mathbb{N}^{\mathbb{S}} \quad \text{by} \quad [\![\varphi_{\mathsf{P}}]\!]^{\mathbb{S}} = [\![\varphi_{\mathsf{P}}]\!]^* \circ \psi_{\mathbb{N}^k}.$$

Analogously, in the case of the k-ary predicate symbol $\chi_{\mathsf{P}} \in \mathcal{L}_1$, we set:

$$[\![\chi_{\mathsf{P}}]\!]^{\mathbb{S}} : (\mathbb{N}^{\mathbb{S}})^k \to \mathbb{B}^{\mathbb{S}} \quad \text{where} \quad [\![\chi_{\mathsf{P}}]\!]^{\mathbb{S}} = [\![\chi_{\mathsf{P}}]\!]^* \circ \psi_{\mathbb{N}^k}.$$

Finally if $\dot{\neg}\colon \mathbb{B} \to \mathbb{B}$ is the boolean negation, and $\dot{\wedge}, \dot{\vee}, \dot{\to} \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ the binary boolean functions for conjunction, disjunction and implication respectively, then define

$$[\![\neg]\!]^{\mathbb{S}} = \mathcal{S}(\dot{\neg}) \quad \text{and} \quad [\![\wedge]\!]^{\mathbb{S}} = \mathcal{S}(\dot{\wedge}) \circ \psi_{\mathbb{B},\mathbb{B}}$$

and similarly for the other connectives.

Definition 5.1. An *environment* is a finite map $\xi : \mathrm{dom}(\xi) \to \mathbb{N}^{\mathbb{S}}$, where $\mathrm{dom}(\xi) \subseteq \mathit{Var}$, which is the set of variables of type Nat (term variables); if $t \in \mathcal{L}_1$ is a term and $\mathrm{FV}(t) \subseteq \mathrm{dom}(\xi)$, define $[\![t]\!]^{\mathbb{S}}_{\xi}$ inductively:

$$[\![x]\!]^{\mathbb{S}}_{\xi} = \xi(x) \qquad [\![\mathsf{f}(t_1,\dots,t_k)]\!]^{\mathbb{S}}_{\xi} = [\![\mathsf{f}]\!]^{\mathbb{S}}([\![t_1]\!]^{\mathbb{S}}_{\xi},\dots,[\![t_k]\!]^{\mathbb{S}}_{\xi})$$
$$[\![\mathsf{n}]\!]^{\mathbb{S}}_{\xi} = [\![\mathsf{n}]\!]^{\mathbb{S}} \qquad [\![\varphi_{\mathsf{P}}(t_1,\dots,t_k)]\!]^{\mathbb{S}}_{\xi} = [\![\varphi_{\mathsf{P}}]\!]^{\mathbb{S}}([\![t_1]\!]^{\mathbb{S}}_{\xi},\dots,[\![t_k]\!]^{\mathbb{S}}_{\xi})$$

If $A \in \mathcal{L}_1$ is a formula and $\mathrm{FV}(A) \subseteq \mathrm{dom}(\xi)$, define $[\![A]\!]^{\mathbb{S}}_{\xi}$ inductively:

$$[\![\mathsf{Q}(t_1,\dots,t_k)]\!]^{\mathbb{S}}_{\xi} = [\![\mathsf{Q}]\!]^{\mathbb{S}}([\![t_1]\!]^{\mathbb{S}}_{\xi},\dots,[\![t_k]\!]^{\mathbb{S}}_{\xi}) \qquad [\![\neg A]\!]^{\mathbb{S}}_{\xi} = [\![\neg]\!]^{\mathbb{S}}([\![A]\!]^{\mathbb{S}}_{\xi})$$
$$[\![\chi_{\mathsf{P}}(t_1,\dots,t_k)]\!]^{\mathbb{S}}_{\xi} = [\![\chi_{\mathsf{P}}]\!]^{\mathbb{S}}([\![t_1]\!]^{\mathbb{S}}_{\xi},\dots,[\![t_k]\!]^{\mathbb{S}}_{\xi}) \qquad [\![A \star B]\!]^{\mathbb{S}}_{\xi} = [\![\dot{\star}]\!]^{\mathbb{S}}([\![A]\!]^{\mathbb{S}}_{\xi},[\![B]\!]^{\mathbb{S}}_{\xi})$$

for $\star = \wedge, \vee, \to$.

Unraveling the definition we have that for all $s \in \mathbb{S}$:

$$[\![\mathsf{f}(t_1,\dots,t_k)]\!]^{\mathbb{S}}_{\xi}(s) = [\![\mathsf{f}]\!]^{\mathcal{I}_0}([\![t_1]\!]^{\mathbb{S}}_{\xi}(s),\dots,[\![t_1]\!]^{\mathbb{S}}_{\xi}(s))$$

and

$$[\![\varphi_{\mathsf{P}}(t_1,\dots,t_k)]\!]^{\mathbb{S}}_{\xi}(s) = [\![\varphi_{\mathsf{P}}]\!]([\![t_1]\!]^{\mathbb{S}}_{\xi}(s),\dots,[\![t_1]\!]^{\mathbb{S}}_{\xi}(s),s).$$

Similar equations hold in the case of formulas. Note that the equality is not treated as a logical symbol, rather as the corresponding (primitive recursive) predicate of $\mathcal{L}_0$.

If $\vec{\alpha}$ is a k-tuple in $(\mathbb{N}^{\mathbb{S}})^k$, $\vec{x}$ a k-tuple of variables and ξ an environment, we denote by $\xi[\vec{\alpha}/\vec{x}]$ the environment ξ' such that $\mathrm{dom}(\xi') = \mathrm{dom}(\xi) \cup \vec{x}$, $\xi'(x_i) = \alpha_i$ for all $1 \le i \le k$ and $\xi'(y) = \xi(y)$ for all $y \notin \vec{x}$.

PROPOSITION 5.2. *If $t, A \in \mathcal{L}_1$ are a term and a formula respectively and $\vec{x}$ a k-tuple of variables including $\mathrm{FV}(t)$ and $\mathrm{FV}(A)$, then the following are convergent global functions:*

$$\lambda\vec{\alpha} : (\mathbb{N}^{\mathbb{S}})^k.[\![t]\!]^{\mathbb{S}}_{[\vec{\alpha}/\vec{x}]}, \quad \lambda\vec{\alpha} : (\mathbb{N}^{\mathbb{S}})^k.[\![A]\!]^{\mathbb{S}}_{[\vec{\alpha}/\vec{x}]}.$$

PROOF. By a straightforward induction. The only non trivial cases concern $[\![\varphi_{\mathsf{P}}]\!]^{\mathbb{S}}$ and $[\![\chi_{\mathsf{P}}]\!]^{\mathbb{S}}$. By Proposition 3.2 these are global and convergent if $[\![\varphi_{\mathsf{P}}]\!]$ and $[\![\chi_{\mathsf{P}}]\!]$ send tuples $\vec{m}$ of natural numbers into individuals. Let $\sigma : \mathbb{N} \to \mathbb{S}$ be any ω-chain in $\mathbb{S}$. For all $i \in \mathbb{N}$ we have:

$$([\![\varphi_{\mathsf{P}}]\!](\vec{m}) \circ \sigma)(i) = [\![\varphi_{\mathsf{P}}]\!](\vec{m}, \sigma(i)).$$

If for all n and i it is the case that $\mathsf{P}(\vec{m}, n) \notin \sigma(i)$ then $[\![\varphi_{\mathsf{P}}]\!](\vec{m}, \sigma(i))$ is constantly 0 which is the limit trivially; otherwise there exists n' and i_0 such that $\mathsf{P}(\vec{m}, n') \in \sigma(i)$ for all $i \ge i_0$, so that the limit of $[\![\varphi_{\mathsf{P}}]\!](\vec{m}) \circ \sigma$ exists and it is n', which is uniquely determined by the consistency of the $\sigma(i)$.

The case of $[\![\chi_{\mathsf{P}}]\!]$ is similar. □

The relevant consequence of Proposition 5.2 is that the interpretation $[\![\cdot]\!]^{\mathbb{S}}$ is actually in the category $\mathcal{G}$. If $\vec{x} \supseteq \mathrm{FV}(t)$ we write $[\![t]\!]^{\mathbb{S}}$ to denote ambiguously its k-ary instance $\lambda\vec{\alpha} : (\mathbb{N}^{\mathbb{S}})^k.[\![t]\!]^{\mathbb{S}}_{[\vec{\alpha}/\vec{x}]}$ for all $k \geq |\vec{x}|$. Then $[\![t]\!]^{\mathcal{G}} = [\![t]\!]^{\mathbb{S}} \restriction I(\mathbb{N})^k$ is well defined, and similarly for $[\![A]\!]^{\mathcal{G}} = [\![A]\!]^{\mathbb{S}} \restriction I(\mathbb{N})^k$.

The next step is to relate interactive realizers and their prefix points to formulas in $\mathcal{L}_1$.

Definition 5.3 (*Interactive Forcing*). Let $r \in \mathbb{R}$ be a realizer, $\alpha \in I(X)$ and $Y = \{Y_s \mid s \in \mathbb{S}\}$ a family of subsets of X indexed over $\mathbb{S}$. Then r *interactively forces* α *into* Y, written $r \Vdash \alpha : Y$, if for all $s \in \mathit{Prefix}\,(r)$ it is the case that $\alpha(s) \in Y_s$.

In the standard interpretations of arithmetic the semantics of a formula A with (free) variables included into $\vec{x} = x_1, \ldots, x_k$ is a k-ary relation over $\mathbb{N}$, which is the extension of the formula. In our interpretation the *extension* of A is the $\mathbb{S}$-indexed family of sets $\mathit{ext}(A) := \{\mathit{ext}(A)_s \mid s \in \mathbb{S}\}$ where:

$$\mathit{ext}(A)_s := \{\vec{m} \mid |\vec{m}| \geq |\mathrm{FV}(A)| \ \ \& \ \ [\![A]\!]^{\mathcal{G}}(\overrightarrow{\lambda\_.m}, s) = \mathsf{true}\}.$$

Here $\vec{m} = m_1, \ldots, m_k$ is a k-ple of natural numbers and $\overrightarrow{\lambda\_.m} = \lambda\_.m_1, \ldots, \lambda\_.m_k$. We are now in place to define the *interactive forcing* of the formula A in terms of the extension of A.

Definition 5.4 (*Interactive Forcing of a Formula*). Let $r \in \mathbb{R}$ be a realizer, $A \in \mathcal{L}_1$ a formula with $\mathrm{FV}(A) \subseteq \vec{x} = x_1, \ldots, x_k$, and $\vec{\alpha} = \alpha_1, \ldots, \alpha_k \in I(\mathbb{N})$. Then we say that r *interactively forces* $\vec{\alpha}$ *into* A, written $r \Vdash \vec{\alpha} : A(\vec{x})$, if and only if $r \Vdash \langle \alpha_1, \ldots, \alpha_k \rangle : \mathit{ext}(A)$.

The intuitive idea of the forcing relation $r \Vdash \vec{\alpha} : A(\vec{x})$ is that, whenever the variables $\vec{x}$ including all the free variables of A are interpreted by the individuals $\vec{\alpha}$, the sequence generated by r out of an arbitrary s_0 will eventually reach (in a finite number of steps) some state $s \in \mathit{Prefix}\,(r)$ such that $\vec{\alpha}(s) \in \mathit{ext}(A)_s$. In this sense A is the actual goal of r. This is however a subtly complex task: the action of r is to direct $\vec{\alpha}$ into $\mathit{ext}(A)$ by extending the given state; but we must keep in mind that such a search aiming at the target $\mathit{ext}(A)_s$ for some s, moves the target itself (which depends on s) as a side effect. Note also that:

$$\langle \alpha_1, \ldots, \alpha_k \rangle(s) = (\alpha_1(s), \ldots, \alpha_k(s)) \in \mathit{ext}(A)_s \Leftrightarrow [\![A]\!]^{\mathcal{G}}(\overrightarrow{\lambda\_.\alpha(s)}, s) = [\![A]\!]^{\mathcal{G}}(\vec{\alpha}, s) = \mathsf{true}.$$

By the fact that we do not ask that the free variables of A are exactly $\vec{x}$, but only included among them, the sets $\mathit{ext}(A)_s$ contain tuples of different length (thought there is a minimum length which is the cardinality of $\mathrm{FV}(A)$), which implies that if $r \Vdash \vec{\alpha} : A(\vec{x})$ then $r \Vdash \vec{\alpha}, \vec{\beta} : A(\vec{x}, \vec{y})$ for all vectors $\vec{y}$ and $\vec{\beta}$ such that $|\vec{y}| = |\vec{\beta}|$.

5.1. The Interactive Realizability Theorem

We are now in place to establish the main result of the paper, namely the correctness of our interpretation, going through a series of lemmas.

LEMMA 5.5 (SUBSTITUTION LEMMA). *For all* $t, t', A \in \mathcal{L}_1$*, environment* ξ *such that* $\mathrm{FV}(t) \cup \mathrm{FV}(t') \cup \mathrm{FV}(A) \subseteq \mathrm{dom}(\xi)$ *and variable* x*:*

$$[\![t'[t/x]]\!]^{\mathbb{S}}_{\xi} = [\![t']\!]^{\mathbb{S}}_{\xi[[\![t]\!]^{\mathbb{S}}_{\xi}/x]} \quad \textit{and} \quad [\![A[t/x]]\!]^{\mathbb{S}}_{\xi} = [\![A]\!]^{\mathbb{S}}_{\xi[[\![t]\!]^{\mathbb{S}}_{\xi}/x]}.$$

PROOF. By a straightforward induction over t' and A. □

LEMMA 5.6. *Let* $A \in \mathcal{L}_1$*. If* A *is either a non logical axiom of* **PRA***, or (an instance of) a logical axiom of* **IPC***, or an instance of the* (φ)*-axiom, then* $[\![A]\!]^{\mathbb{S}}_{\xi}(s) = \mathsf{true}$ *for any environment* ξ *and state* s*.*

PROOF. If $t, A \in \mathcal{L}_0$ let us write $[\![t]\!]^{\mathcal{I}_0}_{\rho}$ and $[\![A]\!]^{\mathcal{I}_0}_{\rho}$ for the respective interpretations of t and A in the standard model w.r.t. some standard environment $\rho : \mathrm{dom}(\rho) \to \mathbb{N}$ such that $\mathrm{FV}(t) \cup \mathrm{FV}(A) \subseteq \mathrm{dom}(\rho)$. Then an immediate consequence of the interpretation of symbols in $\mathcal{L}_0$ by pointwise lifting of their standard interpretations is that for all environment ξ such that $\mathrm{FV}(t) \cup \mathrm{FV}(A) \subseteq \mathrm{dom}(\xi)$ and $s \in \mathbb{S}$:

$$[\![t]\!]^{\mathbb{S}}_{\xi}(s) = [\![t]\!]^{\mathcal{I}_0}_{\rho_{\xi,s}} \ \text{ and } \ [\![A]\!]^{\mathbb{S}}_{\xi}(s) = [\![A]\!]^{\mathcal{I}_0}_{\rho_{\xi,s}}, \quad \text{where } \mathrm{dom}(\rho_{\xi,s}) = \mathrm{dom}(\xi) \text{ and } \rho_{\xi,s}(x) = \xi(x, s),$$

which can be established by an easy induction over t and A. Now if A is a non logical axiom of **PRA** then $A \in \mathcal{L}_0$ and $[\![A]\!]^{\mathcal{I}_0}_\rho = \mathsf{true}$ for any ρ, thus $[\![A]\!]^{\mathbb{S}}_\xi(s) = [\![A]\!]^{\mathcal{I}_0}_{\rho_{\xi,s}} = \mathsf{true}$ for any ξ and s.

Let $A \in \mathcal{L}_1$ be a logical axiom of **IPC**. Then there exists an axiom A' of **IPC**, the propositional variables $p_1, \dots, p_k$ and the formulas $A_1, \dots, A_k \in \mathcal{L}_1$ such that $A = A'[A_1/p_1, \dots, A_k/p_k]$. If $\eta : \mathit{PropVar} \to \mathbb{B}^{\mathbb{S}}$ is an environment of the propositional letters, then by an obvious extension of Lemma 5.5 to the propositional variables we have:

$$[\![A'[A_1/p_1, \dots, A_k/p_k]]\!]^{\mathbb{S}}_\xi = [\![A']\!]^{\mathbb{S}}_{\xi,\eta} \quad \text{where } \eta(p_i, s) = [\![A_i]\!]^{\mathbb{S}}_\xi(s).$$

The thesis follows by the fact that A' is a tautology.

Eventually let $A \equiv \chi_{\mathsf{P}}(\vec{x}) \to \mathsf{P}(\vec{x}, \varphi_{\mathsf{P}}(\vec{x}))$ be an instance of the (φ)-axiom, where P is a primitive recursive predicate, and let ξ and s be arbitrary environment and state respectively. Then

$$[\![A]\!]^{\mathbb{S}}_\xi(s) = [\![\dot{\to}]\!]^{\mathbb{S}}([\![\chi_{\mathsf{P}}(\vec{x})]\!]^{\mathbb{S}}_\xi, [\![\mathsf{P}(\vec{x}, \varphi_{\mathsf{P}}(\vec{x}))]\!]^{\mathbb{S}}_\xi)(s) = [\![\chi_{\mathsf{P}}(\vec{x})]\!]^{\mathbb{S}}_\xi(s) \dot{\to} [\![\mathsf{P}(\vec{x}, \varphi_{\mathsf{P}}(\vec{x}))]\!]^{\mathbb{S}}_\xi(s).$$

Now if $[\![\chi_{\mathsf{P}}(\vec{x})]\!]^{\mathbb{S}}_\xi(s) = [\![\chi_{\mathsf{P}}]\!](\vec{m}, s) = \mathsf{false}$, where $\vec{m} = m_1, \dots, m_k$ for some k and $m_i = \xi(x_i, s)$ for all $i = 1, \dots, k$, then $[\![A]\!]^{\mathbb{S}}_\xi(s) = \mathsf{true}$ vacuously. Otherwise $\mathsf{P}(\vec{m}, n) \in s$ for some $n \in \mathbb{N}$: this implies that $\mathsf{P}(\vec{m}, n)$ is a fact and that $[\![\varphi_{\mathsf{P}}(\vec{x})]\!]^{\mathbb{S}}_\xi(s) = [\![\varphi_{\mathsf{P}}]\!](\vec{m}, s) = n$, so that $[\![\mathsf{P}(\vec{x}, \varphi_{\mathsf{P}}(\vec{x}))]\!]^{\mathbb{S}}_\xi(s) = [\![\mathsf{P}(\vec{m}, n)]\!]^{\mathcal{I}_0} = \mathsf{true}$. □

COROLLARY 5.7 (ARITHMETICAL, LOGICAL AND (φ) AXIOMS). *If A is either a non logical axiom of* **PRA***, or an axiom of* **IPC***, or an instance of the (φ)-axiom, then $\lambda\_.\bot \Vdash \vec{\alpha} : A$.*

PROOF. By Lemma 5.6, since $\lambda\_.\bot$ is a realizer and $\mathit{Prefix}\,(\lambda\_.\bot) = \mathbb{S}$. □

For any $k+1$-ary primitive recursive predicate P (we abuse notation below, writing ambiguously P for the symbol and for its standard interpretation) let us define $r_{\mathsf{P}} : \mathbb{N}^{k+1} \times \mathbb{S} \to \mathbb{S}$ as follows:

$$r_{\mathsf{P}}(\vec{m}, n, s) = \begin{cases} \{\mathsf{P}(\vec{m}, n)\} & \text{if } \mathsf{P}(\vec{m}, n) \text{ is a fact and } \mathsf{P}(\vec{m}, n') \notin s \text{ for all } n' \\ \bot & \text{else.} \end{cases}$$

LEMMA 5.8. *For all $\vec{m}, n \in \mathbb{N}$, $\lambda s : \mathbb{S}.\ r_{\mathsf{P}}(\vec{m}, n, s)$ is a realizer.*

PROOF. That $r_{\mathsf{P}}(\vec{m}, n, s) \cap s = \bot$ for any $s \in \mathbb{S}$ is immediate by definition. It remains to prove that $\lambda s : \mathbb{S}.\ r_{\mathsf{P}}(\vec{m}, n, s) \in I(\mathbb{N})$ and that r_{P} is consistent with its argument.

Let σ be any ω-chain in $\mathbb{S}$. If $[\![\mathsf{P}(\vec{m}, n)]\!]^{\mathcal{I}_0} = \mathsf{false}$ then $r_{\mathsf{P}}(\vec{m}, n, \sigma(i)) = \bot$ for all i. Suppose instead that $\mathsf{P}(\vec{m}, n)$ is true in $\mathcal{I}_0$, namely that it is a fact. If $\mathsf{P}(\vec{m}, n') \notin \sigma(i)$ for all n' and i, then $r_{\mathsf{P}}(\vec{m}, n, \sigma(i)) = \{\mathsf{P}(\vec{m}, n)\}$ for all i; otherwise there exist i and n' such that for all $j \geq i$, $\mathsf{P}(\vec{m}, n') \in \sigma(j)$, as σ is weakly increasing. Then $r_{\mathsf{P}}(\vec{m}, n, \sigma(j)) = \bot$ for all $j \geq i$.

If $r_{\mathsf{P}}(\vec{m}, n, s) = \{\mathsf{P}(\vec{m}, n)\}$ then $\mathsf{P}(\vec{m}, n)$ is a fact so that $\{\mathsf{P}(\vec{m}, n)\} \in \mathbb{S}$. Moreover $\mathsf{P}(\vec{m}, n') \notin s$ for all $n' \in \mathbb{N}$, hence $\{\mathsf{P}(\vec{m}, n)\} \uparrow s$. If instead $r_{\mathsf{P}}(\vec{m}, n, s) = \bot$ then the thesis holds trivially since $\bot \uparrow s$. □

We define $r^{\mathbb{S}}_{\mathsf{P}} := r^*_{\mathsf{P}} \circ \psi_{\mathbb{N}^{k+1}}$, so that for any $\vec{\alpha}, \beta \in \mathbb{N}^{\mathbb{S}}$ we have:

$$r^{\mathbb{S}}_{\mathsf{P}}(\vec{\alpha}, \beta) = \lambda s : \mathbb{S}.\ r_{\mathsf{P}}(\vec{\alpha}(s), \beta(s), s).$$

LEMMA 5.9 (χ-AXIOM). *If P is a $k+1$-ary primitive recursive predicate, and $\vec{\alpha}, \beta \in I(\mathbb{N})$ then $r^{\mathbb{S}}_{\mathsf{P}}(\vec{\alpha}, \beta)$ is a realizer, and it is such that:*

$$r^{\mathbb{S}}_{\mathsf{P}}(\vec{\alpha}, \beta) \Vdash \vec{\alpha}, \beta : \mathsf{P}(\vec{x}, y) \to \chi_{\mathsf{P}}(\vec{x}).$$

PROOF. By definition, $r^{\mathbb{S}}_{\mathsf{P}}(\vec{\alpha}, \beta, s) = r_{\mathsf{P}}(\vec{\alpha}(s), \beta(s), s)$, so that it is consistent with s and $r^{\mathbb{S}}_{\mathsf{P}}(\vec{\alpha}, \beta, s) \cap s = \bot$ because $r_{\mathsf{P}}(\vec{m}, n, s) \cap s = \bot$ for all $\vec{m}, n$. Since r^*_{P} is global and convergent by Lemma 5.8 and Proposition 3.2, we know that $r^{\mathbb{S}}_{\mathsf{P}}$ is $k+1$-global and convergent. Now

$$r^{\mathbb{S}}_{\mathsf{P}}(\overrightarrow{\lambda\_.m}, \lambda\_.n, s) = r_{\mathsf{P}}(\vec{m}, n, s),$$

and the latter is an individual. It follows that $r^{\mathbb{S}}_{\mathsf{P}}(\vec{\alpha}, \beta)$ is an individual if $\vec{\alpha}$ and β are such. We conclude that $r^{\mathbb{S}}_{\mathsf{P}}(\vec{\alpha}, \beta)$ is a realizer.

If $s \in \mathit{Prefix}\,(r^{\mathbb{S}}_{\mathsf{P}}(\vec{\alpha},\beta))$ then $r_{\mathsf{P}}(\vec{\alpha}(s),\beta(s),s) = \bot$. It follows that either $\mathsf{P}(\vec{\alpha}(s),\beta(s))$ is not a fact or $\mathsf{P}(\vec{\alpha}(s),n) \in s$ for some $n \in \mathbb{N}$ (not necessarily equal to $\beta(s)$): this implies that $[\![\chi_{\mathsf{P}}(\vec{x})]\!]^{\mathbb{S}}_{[\vec{\alpha},\beta/\vec{x},y]}(s) = [\![\chi_{\mathsf{P}}]\!](\vec{\alpha}(s),s) = \mathsf{true}$. In both cases we have:

$$[\![\mathsf{P}(\vec{x},y) \to \chi_{\mathsf{P}}(\vec{x})]\!]^{\mathbb{S}}_{[\vec{\alpha},\beta/\vec{x},y]}(s) = [\![\mathsf{P}(\vec{x},y) \to \chi_{\mathsf{P}}(\vec{x})]\!]^{\mathcal{G}}(\vec{\alpha},\beta,s) = \mathsf{true},$$

that is $\vec{\alpha}(s),\beta(s) \in \mathit{ext}(\mathsf{P}(\vec{x},y) \to \chi_{\mathsf{P}}(\vec{x}))_s$. □

LEMMA 5.10 (MODUS PONENS RULE). *If $r \Vdash \vec{\alpha} : A$ and $r' \Vdash \vec{\alpha} : A \to B$ then $r \bullet^{\mathcal{S}} r' \Vdash \vec{\alpha} : B$.*

PROOF. Let $\vec{\alpha} = \alpha_1,\dots,\alpha_k$: then $\mathit{ext}(A \to B)_s, \mathit{ext}(A)_s$ and $\mathit{ext}(B)_s$ are subsets of the universe $\bigcup_k \mathbb{N}^k$, so that in particular we can take the complement $\overline{\mathit{ext}(A)_s} = \bigcup_k \mathbb{N}^k \setminus \mathit{ext}(A)_s$. Then let us observe that for all $s \in \mathbb{S}$:

$$\mathit{ext}(A \to B)_s = \overline{\mathit{ext}(A)_s} \cup \mathit{ext}(B)_s.$$

By Proposition 4.7 we know that $r \bullet^{\mathcal{S}} r'$ is a realizer such that $\mathit{Prefix}\,(r \bullet^{\mathcal{S}} r') = \mathit{Prefix}\,(r) \cap \mathit{Prefix}\,(r')$. Therefore, by the hypotheses, if $s \in \mathit{Prefix}\,(r \bullet^{\mathcal{S}} r')$ then

$$\vec{\alpha}(s) \in \mathit{ext}(A)_s \cap \mathit{ext}(A \to B)_s = \mathit{ext}(A)_s \cap (\overline{\mathit{ext}(A)_s} \cup \mathit{ext}(B)_s) = \mathit{ext}(A)_s \cap \mathit{ext}(B)_s \subseteq \mathit{ext}(B)_s,$$

hence $\vec{\alpha}(s) \in \mathit{ext}(B)_s$ as desired. □

In the next lemma by writing $A(x)$ we mean that x might occur free in A, and $A(t)$ is informal for the substitution $A[t/x]$ of t for x in A.

LEMMA 5.11 (SUBSTITUTION RULE). *If $r \Vdash \vec{\alpha},\beta : A(\vec{x},y)$ for all $\vec{\alpha},\beta \in I(\mathbb{N})$, then for any $t \in \mathcal{L}_1$ such that $\mathrm{FV}(t) \subseteq \vec{x}$, $r \Vdash \vec{\alpha},\beta : A(\vec{x},t)$.*

PROOF. By the hypothesis and the fact that $[\![t]\!]^{\mathbb{S}}_{[\vec{\alpha}/\vec{x}]} = [\![t]\!]^{\mathcal{G}}(\vec{\alpha})$ is an individual by Proposition 5.2, we have that $r \Vdash \vec{\alpha},[\![t]\!]^{\mathbb{S}}_{[\vec{\alpha}/\vec{x}]} : A(\vec{x},y)$, where we note that the environment $[\vec{\alpha}/\vec{x}]$ is not defined over y, which however does not occur in t. By Lemma 5.5

$$[\![A(\vec{x},y)]\!]^{\mathbb{S}}_{[\vec{\alpha},[\![t]\!]^{\mathbb{S}}_{\vec{\xi}}/\vec{x},y]} = [\![A(\vec{x},t)]\!]^{\mathbb{S}}_{[\vec{\alpha}/\vec{x}]},$$

so that $r \Vdash \vec{\alpha} : A(\vec{x},t)$ and, since $y \notin \mathrm{FV}(A(\vec{x},t))$, also $r \Vdash \vec{\alpha},\beta : A(\vec{x},t)$. □

LEMMA 5.12 (INDUCTION RULE). *Suppose that for all $\vec{\alpha},\beta \in I(\mathbb{N})$:*

$$r(\vec{\alpha}) \Vdash \vec{\alpha} : A(x,0) \quad \textit{and} \quad r'(\vec{\alpha},\beta) \Vdash \vec{\alpha},\beta : A(x,y) \to A(\vec{x},\mathsf{succ}(y)).$$

For all $\vec{\alpha}$ let $f(\vec{\alpha}) : \mathbb{N} \to \mathbb{S}^{\mathbb{S}}$ be defined by (primitive) recursion: $f(\vec{\alpha},0) = \lambda\_.\bot$ and $f(\vec{\alpha},n+1) = f(\vec{\alpha},n) \bullet^{\mathcal{S}} r'(\vec{\alpha},\lambda\_.n)$. Then for all individuals $\vec{\alpha}$ and β, $f(\vec{\alpha})^*(\beta) \in \mathbb{R}$ and:

$$r \bullet^{\mathcal{S}} (f(\vec{\alpha})^*(\beta)) \Vdash \vec{\alpha},\beta : A(x,y).$$

PROOF. To simplify the notation, we fix the vector $\vec{\alpha}$ and write just r for $r(\vec{\alpha})$, $r'(\beta)$ for $r'(\vec{\alpha},\beta)$, $f(n)$ for $f(\vec{\alpha},n)$ and hence $f^*(\beta)$ for $f(\vec{\alpha})^*(\beta)$.

First we have to check that $f^*(\beta)$ is a realizer. Note that for any $n \in \mathbb{N}$ we have $f^*(\lambda\_.n) = r'(\lambda\_.0) \bullet^{\mathcal{S}} \cdots \bullet^{\mathcal{S}} r'(\lambda\_.n-1)$ (or just $\lambda\_.\bot$ when $n = 0$), which is a realizer by Proposition 4.7. The function $f^*(\beta)$ is global (or k-global to take the $\vec{\alpha}$ into account) by Proposition 3.2 and, as we have just seen, it sends constant individuals into realizers which are individuals of $\mathbb{S}$: hence $f^*(\beta)$ is an individual for any individual β by Theorem 3.3. The remaining conditions (2) and (3) of Definition 4.1 are immediately seen to hold by observing that for all $s \in \mathbb{S}$, $f^*(\beta,s) = r'(\lambda\_.0,s) \bullet \cdots \bullet r'(\lambda\_.\beta(s)-1,s)$.

In order to prove the thesis, we establish by induction over n that:

$$\forall n \in \mathbb{N}.\ r \bullet^{\mathcal{S}} f^*(\lambda\_.n) \Vdash \vec{\alpha},\lambda\_.n : A(x,y). \tag{4}$$

For the base case we have $r \bullet^{\mathcal{S}} f^*(\lambda\_.0) = r \bullet^{\mathcal{S}} \lambda\_.\bot = r$, and we know that $r \Vdash \vec{\alpha} : A(x,0)$, which implies $r \Vdash \vec{\alpha},\lambda\_.0 : A(x,0)$ vacuously as $y \notin \mathrm{FV}(A)$.

For the step case we have $r \bullet^{\mathcal{S}} f^*(\lambda\_.n+1) = r \bullet^{\mathcal{S}} f^*(\lambda\_.n) \bullet^{\mathcal{S}} r'(\lambda\_.n)$, but:

$$r'(\lambda\_.n) \Vdash \vec{\alpha}, \lambda\_.n : A(x,y) \to A(\vec{x}, \mathsf{succ}(y)) \text{ by the hypothesis of the lemma, and}$$

$$r \bullet^{\mathcal{S}} f^*(\lambda\_.n) \Vdash \vec{\alpha}, \lambda\_.n : A(x,y) \text{ by induction hypothesis.}$$

We then obtain that $r \bullet^{\mathcal{S}} f^*(\lambda\_.n+1) \Vdash \vec{\alpha}, \lambda\_.n : A(x, \mathsf{succ}(y))$, by Lemma 5.10. By the Substitution Lemma 5.5, $[\![A(x,\mathsf{succ}(y))]\!]^{\mathbb{S}}_{[\vec{\alpha},\lambda\_.n/\vec{x},y]} = [\![A(x,y)]\!]^{\mathbb{S}}_{[\vec{\alpha},\lambda\_.n+1/\vec{x},y]}$, and therefore we conclude that $r \bullet^{\mathcal{S}} f^*(\lambda\_.n+1) \Vdash \vec{\alpha}, \lambda\_.n+1 : A(x,y)$.

Now for any $\beta \in \mathcal{S}\mathbb{N}$ and $s \in \mathbb{S}$:

$$(r \bullet^{\mathcal{S}} f^*(\beta))(s) = r(s) \bullet f^*(\beta, s) = r(s) \bullet f^*(\lambda\_.\beta(s), s),$$

because f^* is global, and $r \bullet^{\mathcal{S}} f^*(\lambda\_.\beta(s)) \Vdash \vec{\alpha}, \lambda\_.\beta(s) : A(x,y)$ by (4) above since $\beta(s) \in \mathbb{N}$. It follows that if $s \in \mathit{Prefix}\,(r \bullet^{\mathcal{S}} f^*(\beta))$ then

$$(r \bullet^{\mathcal{S}} f^*(\beta))(s) = \bot = (r \bullet^{\mathcal{S}} f^*(\lambda\_.\beta(s)))(s),$$

so that $s \in \mathit{Prefix}\,(r \bullet^{\mathcal{S}} f^*(\lambda\_.\beta(s)))$. This implies that

$$[\![A(x,y)]\!]^{\mathcal{G}}(\vec{\alpha}, \beta, s) = [\![A(x,y)]\!]^{\mathbb{S}}_{[\vec{\alpha},\beta/\vec{x},y]}(s) = [\![A(x,y)]\!]^{\mathbb{S}}_{[\vec{\alpha},\lambda\_.\beta(s)/\vec{x},y]}(s) = \mathsf{true}$$

as desired. □

THEOREM 5.13 (INTERACTIVE REALIZABILITY THEOREM). *Suppose that* Π *is a proof in* $\mathbf{PRA}+\mathbf{EM}_1$ *of a formula* $A \in \mathcal{L}_1$ *with* $\mathrm{FV}(A) \subseteq \vec{x} = x_1, \ldots, x_k$. *Then for all* $\vec{\alpha} = \alpha_1, \ldots, \alpha_k$ *of individuals in* $I(\mathbb{N})$ *there exists a realizer* $r(\vec{\alpha})$ *which is recursive in* $\vec{\alpha}$, *such that* $r(\vec{\alpha}) \Vdash \vec{\alpha} : A$. *Moreover the definition of* $r(\vec{\alpha})$ *depends on the proof* Π.

PROOF. The existence of $r(\vec{\alpha})$ follows by Corollary 5.7, lemmas 5.9, 5.10, 5.11 and 5.12, and by the remark that (possibly after renaming) the length k of $\vec{x}$ and $\vec{\alpha}$ can be taken to be large enough to include all variables occurring in the proof. That r is a recursive functional of $\vec{\alpha}$ follows by the fact that all realizers constructed in the lemmas above are λ-definable if $\bullet^{\mathcal{S}}$ is recursive. Finally that $r(\vec{\alpha})$ (and hence r itself) actually reflects the structure of the proof of A is clear by construction. □

We eventually turn back to the problem of program extraction in $\mathbf{PRA}+\mathbf{EM}_1$.

COROLLARY 5.14 (PROGRAM EXTRACTION FROM PROOFS IN $\mathbf{PRA}+\mathbf{EM}_1$).
Let Π *be a proof of* $A(\vec{x}, t(\vec{x}))$ *in* $\mathbf{PRA}+\mathbf{EM}_1$. *Then there exists a recursive function* p *such that*

$$\forall \vec{m} \in \mathbb{N}\ \exists \mathcal{I} \supseteq \mathcal{I}_0.\ [\![A(\vec{m}, t(\vec{m}))]\!]^{\mathcal{I}} = \mathsf{true}\ \ \&\ \ p(\vec{m}) = [\![t(\vec{m})]\!]^{\mathcal{I}}.$$

PROOF. Let r be obtained from Π as in Theorem 5.13. Then it is recursive if $\bullet^{\mathcal{S}}$, that is $\bullet$, is recursive; $r(\vec{\alpha}) \in \mathbb{R}$ and r is such that for all $\vec{\alpha} \in I(\mathbb{N})$, $r(\vec{\alpha}) \Vdash \vec{\alpha} : A(\vec{x}, t(\vec{x}))$. Consider the recursive functional:

$$R(\vec{\alpha}, s) = \text{if } r(\vec{\alpha}, s) = \bot \text{ then } s \text{ else } R(\vec{\alpha}, s \sqcup r(\vec{\alpha}, s)).$$

Then R is a total functional by Proposition 4.2 and, for any $s_0 \in \mathbb{S}$, it computes the sup of the ω-chain $s_0 \sqsubseteq s_1 = s_0 \sqcup r(\vec{\alpha}, s_0) \sqsubseteq s_2 = s_1 \sqcup r(\vec{\alpha}, s_1) \sqsubseteq \cdots$ which is the least prefix point of the realizer $r(\vec{\alpha})$ greater than s_0. Then given $\vec{m} \in \mathbb{N}$ we set:

$$s' = R(\overrightarrow{\lambda\_.m}, \bot) \quad \text{and} \quad p(\vec{m}) = [\![t(\vec{x})]\!]^{\mathcal{G}}(\overrightarrow{\lambda\_.m}, s').$$

Now take $\mathcal{I} = \mathcal{I}_{s'}$. □

6. CONCLUSIONS AND FURTHER RESEARCH

We have defined a new method to solve the program extraction problem in a non constructive extension of the primitive recursive arithmetic. We have interpreted non-constructive proofs of arithmetical statements which can be obtained by using excluded middle over Σ^0_1 formulas as procedures that learn about their truth by redefining the value of choice functions. The structure of proofs is reflected by their realizers, which are compositional, and parametric in the composition operation.

Hence the proof itself is responsible for the efficiency of the extracted program, which is not a brute force search in general.

The construction we have used is proof theoretic in nature, but it consists of a process to effectively approximate a classical model of the theory $\mathbf{PRA} + \mathbf{EM}_1$: we consider the present work as a step toward a constructive view of classical logic and arithmetic, which have been traditionally understood in model theory rather than in proof theory.

To our knowledge the category $\mathcal{G}$ of individuals and convergent global functions is new. Its construction can be framed into the theory of strong monads as we suggest, and this is true also of interactive realizers and forcing. We have presented a concrete definition of the category, leaving to future investigation the abstract categorical analysis of the involved concepts. From this work we expect a better understanding of interactive forcing w.r.t. both realizability and forcing as known from the semantics of intuitionistic arithmetic.

In [Caff 2010] there is a detailed reconstruction of the example in the Introduction, using to the equivalent but more concise inference rule of well-founded induction instead of ordinary induction. Interactive realizers can be pratically executed using the interpreter described in [Rispoli 2009]. Further work is needed to compare our program extraction method w.r.t. other methods known from the literature, as well as to provide relevant examples of interesting mathematical proofs.

As further steps we envisage the recasting of the (existing) extension of interactive realizers to $\mathbf{HA} + \mathbf{EM}_1$ in the category $\mathcal{G}$ and, more importantly, a generalisation encompassing $\mathbf{EM}_n$ axiom schemata, namely excluded middle of arithmetical formulas of any degree n.

Aknowledgements

The authors are grateful to Eugenio Moggi and Giuseppe Rosolini for kindly discussing about the topic of the present paper. Thanks to Paul Taylor for his diagram and prooftree macros.

REFERENCES

AKAMA, Y., BERARDI, S., HAYASHI, S., AND KOHLENBACH, U. 2004. An arithmetical hierarchy of the law of excluded middle and related principles. In *Proc. of LICS'04*. 192–201.

ASCHIERI, F. 2010. Interactive Learning Based Realizability and 1-Backtracking Games. In *Proceedings of Classical Logic and Computation 2010*. EPTCS. To appear.

ASCHIERI, F. 2011. Learning, realizability, games and classical logic. PhD Thesis.

ASCHIERI, F. AND BERARDI, S. 2010. Interactive Learning-Based Realizability for Heyting Arithmetic with EM_1. *Logical Methods in Computer Science 6,* 3.

BERARDI, S. 2005. Classical logic as limit completion. *Mathematical Structures in Computer Science 15,* 1, 167–200.

BERARDI, S., COQUAND, T., AND HAYASHI, S. 2005. Games with 1-backtracking. In *GALOP*, D. R. Ghica and G. McCusker, Eds. 210–225. submitted to APAL.

BERARDI, S. AND DE' LIGUORO, U. 2009. Toward the interpretation of non-constructive reasoning as non-monotonic learning. *Information and Computation 207,* 1, 63–81.

BERARDI, S. AND DE'LIGUORO, U. 2008. A Calculus of Realizers for EM_1 Arithmetic (Extended Abstract). In *CSL*. LNCS, vol. 5213. 215–229.

CAFF, S. 2010. Costruzione di realizzatori interattivi da prove in PRA+EM_1 ed estrazione da Isabelle/HOL. Master Thesis.

COQUAND, T. 1995. A semantics of evidence for classical arithmetic. *J. Symb. Log. 60*, 325–337.

CROLE, R. L. 1993. *Categories for Types*. Cambridge University Press.

GOLD, E. M. 1965. Limiting recursion. *J. Symb. Log. 30*, 28–48.

GOLD, E. M. 1967. Language identification in the limit. *Information and Control 10*, 447–474.

HAYASHI, S. 2006. Mathematics based on incremental learning, excluded middle and inductive inference. *Theor. Comp. Sci. 350*, 125–139.

HILBERT, D. AND BERNAYS, P. 1970. *Grundlagen der Mathematik*. Vol. II. Springer.

MOGGI, E. 1991. Notions of computation and monads. *Inf. Comput. 93,* 1, 55–92.

RISPOLI, D. 2009. An implementation of interactive realizers for classical arithmetic without nested quantiers. Master Thesis.

TROELSTRA, A. S. AND VAN DALEN, D. 1988. *Constructivism in Mathematics*. Vol. 1, 2. North-Holland.

Received May 2010; revised November 2010; accepted January 2011