Open access • Journal Article • DOI:10.1017/S0960129501003358

# Extracting information from intermediate semiconstructive HA-systems – extended abstract — Source link

Mauro Ferrari, Camillo Fiorentini, Pierangelo Miglioli

**Institutions:** University of Milan

**Published on:** 01 Aug 2001 - Mathematical Structures in Computer Science (Cambridge University Press)

**Topics:** Program synthesis, Formal verification and Mathematical proof


# Extracting information from intermediate semiconstructive HA-systems – extended abstract


MAURO FERRARI, CAMILLO FIORENTINI and PIERANGELO MIGLIOLI



Mathematical Structures in Computer Science / Volume 11 / Issue 04 / August 2001, pp 589 - 596
DOI: 10.1017/S0960129501003358, Published online: 25 July 2001

*Math. Struct. in Comp. Science* (2001), *vol.* 11, *pp.* 589–596. Printed in the United Kingdom


# Extracting information from intermediate semiconstructive HA-systems – extended abstract†

MAURO FERRARI, CAMILLO FIORENTINI
and PIERANGELO MIGLIOLI

*Università degli Studi di Milano, Dipartimento di Scienze dell'Informazione, via Comelico 39, 20135 Milano, Italy*

*Received 1 October 1999; revised 15 May 2000*

In this abstract we will describe research in progress on the problem of extracting information from proofs. Here we will concentrate our attention on semiconstructive calculi, which is a kind of calculus that is of interest in the framework of program synthesis and formal verification. We will discuss the notion of uniformly semiconstructive calculus, introduce our information extraction mechanism and apply it to two calculi extending Intuitionistic Arithmetic.

## 1. Introduction

In previous work (Ferrari 1997; Ferrari *et al.* 1999a; Ferrari *et al.* 1999b; Ferrari *et al.* 2000) the authors have developed a method for extracting information from proofs of constructive systems that also works in cases where the usual information extraction techniques based on Normalization, Cut-elimination or Realizability cannot be applied.

In this abstract we describe how our technique can be extended to handle 'weaker' systems, which we call *semiconstructive*. Formally, a system $\mathbf{T} \oplus \mathbf{L}$, where $\mathbf{T}$ is a first order theory (the mathematical part) and $\mathbf{L}$ is a super-intuitionistic logic (the deductive apparatus) is *semiconstructive* if it satisfies the *weak disjunction property* (if a closed wff $A \vee B$ belongs to $\mathbf{T} \oplus \mathbf{L}$, then either $A$ or $B$ belongs to the corresponding classical theory $\mathbf{T} \oplus \mathbf{Cl}$) and the *weak explicit definability property* (if a closed wff $\exists x A(x)$ belongs to $\mathbf{T} \oplus \mathbf{L}$, then $A(t)$ belongs to the corresponding classical theory $\mathbf{T} \oplus \mathbf{Cl}$ for some closed term $t$). The notion of semiconstructive system is relevant in the context of the authors' approach to program synthesis, formal verification and Abstract Data Types specification (Miglioli and Ornaghi 1981; Miglioli *et al.* 1989; Miglioli *et al.* 1994; Avellone *et al.* 1999; Benini 1999). Indeed, if $\mathbf{T}$ is a theory completely formalizing an Abstract Data Type, according to the characterization of Abstract Data Types based on the notion of *isoinitial model* (Miglioli *et al.* 1994), the addition of $\mathbf{T}$ to a semiconstructive deductive apparatus $\mathbf{L}$ gives rise to a recursively axiomatizable and semiconstructive system $\mathbf{T} \oplus \mathbf{L}$.

† The full version of this paper is available at `http://homes.dsi.unimi.it/~ferram`

Therefore, if $\mathbf{T} \oplus \mathbf{L}$ contains a proof $\pi$ of a formula $\forall \underline{x} \exists ! y A(\underline{x}, y)$ (respectively, a formula of the kind $\forall \underline{x}(B(\underline{x}) \vee \neg B(\underline{x}))$), then the whole system $\mathbf{T} \oplus \mathbf{Cl}$ can be used to compute the function (respectively, the predicate) associated with such a formula (Miglioli *et al.* 1989; Miglioli *et al.* 1994). If the system $\mathbf{T} \oplus \mathbf{L}$ does not satisfy further properties, the algorithm to compute the function (the predicate) is highly inefficient since it does not use the 'local' information contained in the proof $\pi$ (the proof $\pi$ is only used to guarantee the termination of the algorithm). Moreover, in general the usual extraction techniques based on Normalization and Realizability cannot be applied to these systems. However, the definition of uniformly semiconstructive calculus guarantees that the function (the predicate) related to the proof $\pi$ can be computed by searching a calculus, the *extraction calculus for* $\pi$, whose proofs are generated starting from the formulas contained in $\pi$; the proofs of the extraction calculus have a bounded logical complexity depending on $\pi$.

## 2. Preliminaries

We use **Int** (**Cl**) to denote the set of intuitionistically (classically) valid formulas (wff's for short) of the pure first-order language $\mathscr{L}^{\dagger}$. A *(first-order) intermediate pseudo-logic* is any set of wff's **L** such that $\mathbf{Int} \subseteq \mathbf{L} \subseteq \mathbf{Cl}$ and **L** is closed under *modus ponens* and generalization. An *intermediate logic* **L** is an intermediate pseudo logic closed under predicate substitution, see, for example, Ono (1972). Given an extra-logical alphabet $\Sigma$, we use $\mathscr{L}_{\Sigma}$ to denote the language generated by $\Sigma$. $\mathbf{Int}_{\Sigma}$ ($\mathbf{Cl}_{\Sigma}$) is the subset of $\mathscr{L}_{\Sigma}$ obtained by correctly substituting the predicate variables with wff's of $\mathscr{L}_{\Sigma}$ in the wff's of **Int** (**Cl**). A pseudo-logic $\mathbf{L}_{\Sigma}$ will be any subset of $\mathscr{L}_{\Sigma}$ such that $\mathbf{Int}_{\Sigma} \subseteq \mathbf{L}_{\Sigma} \subseteq \mathbf{Cl}_{\Sigma}$ and $\mathbf{L}_{\Sigma}$ is closed under *modus ponens* and generalization. Finally, if $\Gamma$ is a set of classically valid wff's of $\mathscr{L}_{\Sigma}$, we use $\Gamma \oplus \mathbf{L}$ to denote the smallest set of wff's (which is an intermediate pseudo-logic) closed under *modus ponens* and generalization that contains the intermediate pseudo-logic **L** and $\Gamma$. Given a $\Sigma$-theory **T** (that is, a recursively enumerable set of classically consistent wff's of $\mathscr{L}_{\Sigma}$), we use *(intermediate)* **T**-*system* to mean any set $\mathbf{S} \subseteq \mathscr{L}_{\Sigma}$ such that $\mathbf{T} \oplus \mathbf{Int} \subseteq \mathbf{S} \subseteq \mathbf{T} \oplus \mathbf{Cl}$ and **S** is closed under *modus ponens* and generalization.

Given $\Gamma, \Delta \subseteq \mathscr{L}_{\Sigma}$ such that $\Gamma \subseteq \Delta$, we have $\Gamma$ is *semiconstructive in* $\Delta$ iff the *weak disjunction property* (wDP) and the *weak explicit definability property* (wED) hold:

— (wDP): if $A \vee B \in \Gamma$ and $A \vee B$ is a closed wff, then either $A \in \Delta$ or $B \in \Delta$.
— (wED): if $\exists x A(x) \in \Gamma$ and $\exists x A(x)$ is a closed wff, then $A(t/x) \in \Delta$ for some closed term $t$ of the language.

We simply say that a **T**-system **S** is *semiconstructive* if **S** is semiconstructive in $\mathbf{T} \oplus \mathbf{Cl}$.

The usual characterization of *constructive* **T**-*system* can be obtained by imposing $\Gamma = \Delta$ in (wDP) and (wED).

## 3. The information extraction mechanism

In this section we will provide a short presentation of our mechanism for extracting information from proofs; for a complete discussion see Ferrari *et al.* (1999b) and Ferrari

[†] The set of logical constants is $\{\bot, \wedge, \vee, \rightarrow, \forall, \exists\}$ and $\neg A$ is an abbreviation for $A \rightarrow \bot$.

*et al.* (2000). Our extraction mechanism is based on an abstract definition of the notions of proof and calculus that allows us to treat extraction from Gentzen, Tableau or Hilbert style calculi

A (single-conclusion) *sequent* is an expression $\Gamma \vdash A$, where $A$ is a wff and $\Gamma$ is a finite set of wff's. A *proof* on $\mathscr{L}_\Sigma$ is any finite object $\pi$ such that:

(1) The (finite) set of wff's of $\mathscr{L}_\Sigma$ occurring in $\pi$ is uniquely determined and nonempty;
(2) $\pi$ proves a sequent $\Gamma \vdash A$, where $\Gamma$ (possibly empty) is the set of *assumptions* of $\pi$, while $A$ is the *consequence* of $\pi$[†].

The notation $\pi : \Gamma \vdash A$ means that $\Gamma \vdash A$ is the sequent proved by $\pi$, and $\mathrm{dg}(\pi)$ denotes the *degree of* $\pi$, that is, the maximum among the degrees of the wff's occurring in $\pi$, where the degree of a wff is defined as usual.

A *calculus* on $\mathscr{L}_\Sigma$ is a pair $(\mathbf{C}, [\cdot])$, where $\mathbf{C}$ is a recursive set of proofs on the language $\mathscr{L}_\Sigma$ and $[\cdot]$ is a recursive map associating with every proof of the calculus the set of its *relevant* subproofs. We require $[\cdot]$ to satisfy the following natural conditions:

(1) $\pi \in [\pi]$;
(2) for every $\pi' \in [\pi]$, $[\pi'] \subseteq [\pi]$;
(3) for every $\pi' \in [\pi]$, $\mathrm{dg}(\pi') \leqslant \mathrm{dg}(\pi)$.

We remark that any usual single conclusion inference system is a calculus according to our definition. In particular, the natural deduction calculi we will use in this paper meet this characterization.

Given $\Pi \subseteq \mathbf{C}$, $\mathrm{Seq}(\Pi) = \{\Gamma \vdash A \mid \pi : \Gamma \vdash A \in \Pi\}$ is the set of the *sequents proved in* $\Pi$; $\mathrm{Theo}(\Pi) = \{A \mid \vdash A \in \mathrm{Seq}(\Pi)\}$ is the set of *theorems proved in* $\Pi$, and $[\Pi] = \{\pi' \mid$ there exists $\pi \in \Pi$ such that $\pi' \in [\pi]\}$ is the *closure under subproofs* of $\Pi$ in the calculus $\mathbf{C}$.

In the following we will be interested in characterizing subsets of a calculus that have some closure properties, and to this end we introduce the notion of generalized rule. Given a language $\mathscr{L}_\Sigma$, let $\Xi$ be the set of all the sequents on $\mathscr{L}_\Sigma$ and let $\Xi^*$ be the set of all the finite sequences of sequents in $\Xi$ ($\epsilon$ denoting the empty sequence); a *generalized rule* is a relation $\mathscr{R} \subseteq \Xi^* \times \Xi$. We will write $\sigma \in \mathscr{R}(\sigma^*)$ as a shorthand for $(\sigma^*, \sigma) \in \mathscr{R}$.

Examples of generalized rules that we will use in the following are:

— *Substitution rule* SUBST: its domain is the set of all the sequents, and, for every substitution $\theta$, $\theta\Gamma \vdash \theta\Delta \in \mathrm{SUBST}(\Gamma \vdash \Delta)$.
— *Cut rule* CUT: its domain contains all the sequences of sequents of the kind $\Gamma_1 \vdash H; \Gamma_2, H \vdash A$, and $\Gamma_1, \Gamma_2 \vdash A \in \mathrm{CUT}(\Gamma_1 \vdash H; \Gamma_2, H \vdash A)$.

A generalized rule $\mathscr{R}$ is an *extraction rule for* $\mathbf{C}$ (*e-rule* for short) with respect to a positive integer $h$ and a function $\phi : \mathbf{N} \to \mathbf{N}$ if:

1 For every $\sigma \in \mathscr{R}(\sigma_1; \ldots; \sigma_n)$ and $\pi_1 : \sigma_1, \ldots, \pi_n : \sigma_n \in \mathbf{C}$, there exists a proof $\pi : \sigma \in \mathbf{C}$ such that $\mathrm{dg}(\pi) \leqslant \max\{\mathrm{dg}(\pi_1), \ldots, \mathrm{dg}(\pi_n), \phi(\mathrm{dg}(\sigma_1)), \ldots, \phi(\mathrm{dg}(\sigma_n)), \phi(\mathrm{dg}(\sigma))\}$.
2 For every $\sigma \in \mathscr{R}(\epsilon)$, $\mathrm{dg}(\sigma) \leqslant h$. For every $\sigma, \sigma_1, \ldots, \sigma_n$ such that $\sigma \in \mathscr{R}(\sigma_1; \ldots; \sigma_n)$, the degree of $\sigma$ is bounded by the degrees of $\sigma_1, \ldots, \sigma_n$.

[†] In general sets of conclusions instead of a single conclusion could be considered.

It is easy to check that SUBST and CUT are e-rules (with respect to a linear function) for the usual natural deduction calculus for Intuitionistic Logic.

Now, given a recursive e-rule $\mathscr{R}$ and a recursive set $\Pi$ of proofs of $\mathbf{C}$, the *extraction calculus* $\mathbb{ID}(\mathscr{R}, \Pi)$ *for* $\Pi$ is defined as follows:

1 If $\sigma \in \mathrm{Seq}(\Pi)$, then $\tau \equiv \sigma$ is a proof-tree of $\mathbb{ID}(\mathscr{R}, \Pi)$.

2 If $\tau_1 : \sigma_1, \ldots, \tau_n : \sigma_n$ are proof-trees of $\mathbb{ID}(\mathscr{R}, \Pi)$, then, for every $\sigma \in \mathscr{R}(\sigma_1; \ldots; \sigma_n)$, the proof-tree

$$\tau \equiv \frac{\tau_1 : \sigma_1 \ \ldots \ \tau_n : \sigma_n}{\sigma}\mathscr{R}$$

belongs to $\mathbb{ID}(\mathscr{R}, \Pi)$.

It is easy to prove that if $\Pi$ has a bounded logical complexity, $\mathbb{ID}(\mathscr{R}, \Pi)$ has a bounded logical complexity.

**Definition 3.1.** Let $\mathbf{C}_1 = (C_1, [.]_1)$ and $\mathbf{C}_2 = (C_2, [.]_2)$ be two calculi on the same language $\mathscr{L}_\Sigma$. $\mathbf{C}_1$ is *uniformly semiconstructive* in $\mathbf{C}_2$ iff there exists an e-rule $\mathscr{R}$ for $\mathbf{C}_2$ such that, for every recursive subset $\Pi$ of $\mathbf{C}_1$, $\mathrm{Theo}([\Pi]_1)$ is semiconstructive in $\mathrm{Theo}(\mathbb{ID}(\mathscr{R}, [\Pi]_1))$.

Given two calculi $\mathbf{C}_1$ and $\mathbf{C}_2$ generating, respectively, a $\mathbf{T}$-system $\mathbf{S}$ (that is, $\mathrm{Theo}(\mathbf{C}_1) = \mathbf{S}$) and its classical extension $\mathbf{T} \oplus \mathbf{Cl}$ (that is, $\mathrm{Theo}(\mathbf{C}_2) = \mathbf{T} \oplus \mathbf{Cl}$), we say that $\mathbf{S}$ is *uniformly semiconstructive* if $\mathbf{C}_1$ is uniformly semiconstructive in $\mathbf{C}_2$.

The main feature of uniformly semiconstructive calculi comes from the fact that the information contained in a proof $\pi$ can be 'partially completed' by the extraction calculus $\mathbb{ID}(\mathscr{R}, [\pi]_1)$ within a bounded logical complexity. For example, if $\pi :\vdash \exists x A(x) \in \mathbf{C}_1$, then we can 'semiconstructively complete' the information contained in the proof $\pi$ by means of the calculus $\mathbb{ID}(\mathscr{R}, [\pi]_1)$ that proves a sequent of the kind $\vdash A(t)$ for some closed term $t$. Since $\mathscr{R}$ is admissible in $\mathbf{C}_2$, we are guaranteed on the provability of $A(t)$ in $\mathbf{C}_2$. On the other hand, $A(t)$ is provable in $\mathbf{C}_1$ if $\mathbf{C}_1$ enjoys the stronger property of uniform constructivity, where a calculus $\mathbf{C} = (C, [.])$ is *uniformly constructive* if there exists an e-rule $\mathscr{R}$ for $\mathbf{C}$ such that, for every recursive $\Pi \subseteq \mathbf{C}$, $\mathrm{Theo}(\mathbb{ID}(\mathscr{R}, [\Pi]))$ is constructive. A $\mathbf{T}$-system $\mathbf{S}$ is uniformly constructive if it can be generated by a uniformly constructive calculus $\mathbf{C}$.

Using the latter characterization, the authors have shown in Ferrari *et al.* (1999b) and Ferrari *et al.* (2000) that a wide family of systems $\mathbf{S} = \mathbf{T} + \mathbf{L}$ (where $\mathbf{T}$ is a mathematical theory and $\mathbf{L}$ is a superintuitionistic calculus) are uniformly constructive. Namely, in Ferrari *et al.* (1999b) it is shown that several systems $\mathbf{S}$ involving a Harrop theory $\mathbf{T}$ and superintuitionistic (intermediate) logics $\mathbf{L}$ are uniformly constructive. The most representative principles studied in that paper are: the *Grzegorczyk Principle* $\forall x(A(x) \vee B) \to \forall x A(x) \vee B$ with $x \notin \mathrm{FV}(B)$, the *Kuroda Principle* $\forall x \neg\neg A(x) \to \neg\neg \forall x A(x)$, the *Extended Scott Principle* $(\forall x(\neg\neg A(x) \to A(x)) \to \exists x(A(x) \vee \neg A(x))) \to \exists x(\neg A(x) \vee \neg\neg A(x))$, the *Kreisel–Putnam Principle* $(\neg A \to B \vee C) \to (\neg A \to B) \vee (\neg A \to C)$ and the *Independence of Premises Principle* $(\neg A \to \exists x B(x)) \to \exists x(\neg A \to B(x))$ with $x \notin \mathrm{FV}(A)$.

On the other hand, in Ferrari *et al.* (1999a) the authors have considered systems $\mathbf{S}$ involving *Hereditary Harrop Theories*, *Grzegorczyk Principle* and the *Descending Chain Principle* $\exists x A(x) \wedge \forall y(A(y) \to \exists z((A(z) \wedge z < y) \vee B)) \to B$, showing that in such cases goal-oriented e-rules can be applied to define the extraction calculus.

## 4. Uniformly semiconstructive HA-systems

Now, let us use $\mathscr{ND}_{\mathbf{HA}}$ and $\mathscr{ND}_{\mathbf{PA}}$ to denote the usual natural deduction calculi for Intuitionistic and Classical Arithmetic respectively (Troelstra 1973). From now on we will investigate the uniform semiconstructivity of two calculi including $\mathscr{ND}_{\mathbf{HA}}$. The related **HA**-systems are particularly interesting since they cannot be extended in fully constructive **HA**-systems and they contain principles that, as far as we know, cannot be treated by the usual information extraction techniques based on Normalization, Cut elimination or Realizability.

Let $\mathbf{HA}^{+}$ be the system obtained by adding to Intuitionistic Arithmetic **HA** the principles: $(\mathrm{Kur}) = \forall x \neg\neg A(x) \to \neg\neg \forall x A(x)$, $(\mathrm{KP}_{\vee}) = (\neg A \to B \vee C) \to (\neg A \to B) \vee (\neg A \to C)$, $(\mathrm{KP}_{\exists}) = (\neg A \to \exists x B(x)) \to \exists x(\neg A \to B(x))$ and $(\mathrm{wGrz}) = \forall x \neg\neg A(x) \wedge \forall x(A(x) \vee B) \to \forall x A(x) \vee B$ where $x \notin \mathrm{FV}(B)$. A detailed discussion on the role of such principles can be found in Troelstra (1973), Miglioli *et al.* (1994), Ferrari *et al.* (1999b) and Ferrari *et al.* (2000). We remark that **T**-systems containing the *Kuroda Principle* (Kur) are not in the scope of traditional recursive realizability interpretations such as Kleene's 1945-realizability (Kleene 1945). The above principles can be expressed by the following pseudo-natural deduction rules

$$\frac{\begin{array}{cc}\Gamma_1 & \Gamma_2 \\ \vdots\,{\scriptstyle \pi_1} & \vdots\,{\scriptstyle \pi_2} \\ \forall x \neg\neg A(x) & \forall x(A(x) \vee B)\end{array}}{\forall x A(x) \vee B}\ \mathrm{wGrz} \qquad \frac{\begin{array}{c}\Gamma \\ \vdots\,{\scriptstyle \pi} \\ \forall x \neg\neg A(x)\end{array}}{\neg\neg \forall x A(x)}\ \mathrm{Kur}$$

$$\frac{\begin{array}{c}\Gamma, [\neg A] \\ \vdots\,{\scriptstyle \pi} \\ B \vee C\end{array}}{(\neg A \to B) \vee (\neg A \to C)}\ \mathrm{KP}_{\vee} \qquad \frac{\begin{array}{c}\Gamma, [\neg A] \\ \vdots\,{\scriptstyle \pi} \\ \exists x B(x)\end{array}}{\exists x(\neg A \to B(x))}\ \mathrm{KP}_{\exists}$$

where in the rule wGrz $x \notin \mathrm{FV}(B)$, while wff's between square brackets denote assumptions discharged by the rule application, see Troelstra (1973). Now, let $\mathscr{ND}_{\mathbf{HA}^{+}}$ be the pseudo-natural deduction calculus obtained by adding the above rules to $\mathscr{ND}_{\mathbf{HA}}$. Moreover, let $\mathrm{RHA}^{+}$ be the union of the generalized rules Cut and Subst and of the following generalized rules

$$\begin{array}{ll}
\textsc{Id}: & \vdash x = x \in \textsc{Id}(\epsilon) \quad \Gamma, \Delta \vdash A(t') \in \textsc{Id}(\Gamma \vdash A(t); \Delta \vdash t = t') \\
\textsc{Sum}: & \vdash x + 0 = x \in \textsc{Sum}(\epsilon) \quad \vdash x + Sy = S(x + y) \in \textsc{Sum}(\epsilon) \\
\textsc{Prod}: & \vdash x * 0 = 0 \in \textsc{Prod}(\epsilon) \quad \vdash x * Sy = x * y + x \in \textsc{Prod}(\epsilon) \\
\textsc{Rkp}\vee: & \Gamma, \Delta \vdash \neg A \to B \in \textsc{Rkp}\vee(\Gamma \vdash B; \Delta \vdash (\neg A \to B) \vee (\neg A \to C)) \text{ with } \neg A \notin \Gamma \\
& \Gamma, \Delta \vdash \neg A \to B \in \textsc{Rkp}\vee(\Gamma, \neg A \vdash B; \Delta \vdash (\neg A \to B) \vee (\neg A \to C)) \\
& \Gamma, \Delta \vdash \neg A \to C \in \textsc{Rkp}\vee(\Gamma \vdash C; \Delta \vdash (\neg A \to B) \vee (\neg A \to C)) \text{ with } \neg A \notin \Gamma \\
& \Gamma, \Delta \vdash \neg A \to C \in \textsc{Rkp}\vee(\Gamma, \neg A \vdash C; \Delta \vdash (\neg A \to B) \vee (\neg A \to C)) \\
& \neg B \vdash \neg B \in \textsc{Rkp}\vee(\Delta \vdash (\neg A \to \neg B) \vee (\neg A \to C)) \\
& \neg C \vdash \neg C \in \textsc{Rkp}\vee(\Delta \vdash (\neg A \to B) \vee (\neg A \to \neg C)) \\
\textsc{Rkp}\exists: & \Gamma, \Delta \vdash \neg A \to B(t) \in \textsc{Rkp}\exists(\Gamma \vdash B(t); \Delta \vdash \exists x(\neg A \to B(x))) \quad \text{with } \neg A \notin \Gamma \\
& \Gamma, \Delta \vdash \neg A \to B(t) \in \textsc{Rkp}\exists(\Gamma, \neg A \vdash B(t); \Delta \vdash \exists x(\neg A \to B(x))) \\
& \neg B(t) \vdash \neg B(t) \in \textsc{Rkp}\exists(\Delta \vdash \exists x(\neg A \to B(x))) \\
\textsc{Rcl}: & \Gamma \vdash \forall x A(x) \in \textsc{Rcl}(\Gamma \vdash \forall x \neg\neg A(x))
\end{array}$$

It is easy to check that $\mathrm{RHA}^{+}$ is an e-rule for $\mathscr{ND}_{\mathbf{PA}}$. Let us use $\mathbb{ID}_{\mathbf{HA}^{+}}([\Pi])$ to denote the abstract calculus $\mathbb{ID}(\mathrm{RHA}^{+}, \mathrm{Seq}([\Pi]))$.

The proof of uniform semiconstructivity can be carried out using the notion of Neg-evaluation. Let $\Pi$ be a set of proofs on $\mathscr{L}_{\mathscr{A}}$, and let Neg and $A$ be a set of closed negated

wff's and a wff in the language $\mathscr{L}_{\mathscr{A}}$, respectively. $A$ is Neg-*evaluated in* $\Pi$ iff the following conditions hold:

1 Either $A \in \mathrm{Neg}$ or there exists a proof $\pi : \Gamma \vdash A \in \Pi$ with $\Gamma \subseteq \mathrm{Neg}$.
2 For every closed instance $\theta A$ of $A$, one of the following conditions holds:
   (a) $\theta A$ is atomic or negated;
   (b) $\theta A \equiv B \wedge C$, and both $B$ and $C$ are Neg-evaluated in $\Pi$;
   (c) $\theta A \equiv B \vee C$, and either $B$ is Neg-evaluated in $\Pi$ or $C$ is Neg-evaluated in $\Pi$;
   (d) $\theta A \equiv B \to C$, and, for every set $\mathrm{Neg}'$ of closed negated wff's of $\mathscr{L}_{\mathscr{A}}$ such that $\mathrm{Neg}' \supseteq \mathrm{Neg}$, if $B$ is $\mathrm{Neg}'$-evaluated in $\Pi$, then $C$ is $\mathrm{Neg}'$-evaluated in $\Pi$;
   (e) $\theta A \equiv \exists x B(x)$, and $B(t/x)$ is Neg-evaluated in $\Pi$ for some closed term $t$ of $\mathscr{L}_{\mathscr{A}}$;
   (f) $\theta A \equiv \forall x B(x)$, and, for every closed term $t$ of $\mathscr{L}_{\mathscr{A}}$, $B(t/x)$ is Neg-evaluated in $\Pi$.

A set $\Gamma$ of wff's is Neg-evaluated in a set of proofs $\Pi$ if every wff $A \in \Gamma$ is Neg-evaluated in $\Pi$. The main step towards the proof of uniform semiconstructivity of $\mathscr{ND}_{\mathbf{HA}^+}$ is given by the following lemma, which can be proved by induction on the depth of the proofs in $\mathscr{ND}_{\mathbf{HA}^+}$.

**Lemma 4.1.** Let $\Pi$ be any recursive set of proofs of $\mathscr{ND}_{\mathbf{HA}^+}$ and let Neg be a set of closed negated wff's of $\mathscr{L}_{\mathscr{A}}$. For any proof $\pi : \Gamma \vdash H$ belonging to the closure under substitution of $[\Pi]$, if $\Gamma$ is Neg-evaluated in $\mathbb{ID}_{\mathbf{HA}^+}([\Pi])$, then $H$ is Neg-evaluated in $\mathbb{ID}_{\mathbf{HA}^+}([\Pi])$.

If $A \vee B$ is a closed wff in $\mathrm{Theo}([\Pi])$, there exists a proof $\pi : \vdash A \vee B$ in the closure under substitution of $[\Pi]$. Since the empty set of premises is $\varnothing$-evaluated in $\mathbb{ID}_{\mathbf{HA}^+}([\Pi])$, by Lemma 4.1, it follows that $A \vee B$ is $\varnothing$-evaluated in $\mathbb{ID}_{\mathbf{HA}^+}([\Pi])$, and this immediately implies that one between the sequents $\vdash A$ and $\vdash B$ is provable in $\mathbb{ID}_{\mathbf{HA}^+}([\Pi])$. With a similar argument one can prove that $\mathrm{Theo}([\Pi])$ has the (wED) property with respect to $\mathrm{Theo}(\mathbb{ID}_{\mathbf{HA}^+}([\Pi]))$. Hence, we can conclude that $\mathrm{Theo}([\Pi])$ is semiconstructive in $\mathrm{Theo}(\mathbb{ID}_{\mathbf{HA}^+}([\Pi]))$. Finally, since $\mathrm{RHA}^+$ is an e-rule for $\mathscr{ND}_{\mathbf{PA}}$, we get the following theorem.

**Theorem 4.2.** $\mathscr{ND}_{\mathbf{HA}^+}$ is a uniformly semiconstructive calculus in $\mathscr{ND}_{\mathbf{PA}}$.

Hence, $\mathbf{HA}^+ = \mathrm{Theo}(\mathscr{ND}_{\mathbf{HA}^+})$ is a uniformly semiconstructive **HA**-system. We remark that the notion of evaluation plays only a technical role in proving the uniform semiconstructivity of the above calculus and it is not related to the extraction mechanism. Finally, to conclude the presentation of this example, we note that the above calculus is uniformly semiconstructive but it is 'essentially' non-constructive. Indeed, we have the following theorem.

**Theorem 4.3.** There exists no consistent and recursively axiomatizable constructive **T**-system **S** such that $\mathbf{HA} \subseteq \mathbf{T}$ and $\mathbf{HA}^+ \subseteq \mathbf{S}$.

Now, let $\mathbf{HA}^{++}$ be the **HA**-system obtained by adding to Intuitionistic Arithmetic the *Markov Principle* $(\mathrm{Mk}) = \forall x(A(x) \vee \neg A(x)) \wedge \neg\neg \exists x A(x) \to \exists x A(x)$ (Troelstra 1973; Miglioli and Ornaghi 1981) and $(\mathrm{DT}) = \exists x A(x) \vee \forall x(A(x) \to B \vee \neg B)$.

$\mathscr{ND}_{\mathbf{HA}^{++}}$ will denote the calculus for $\mathbf{HA}^{++}$ obtained by adding to $\mathscr{ND}_{\mathbf{HA}}$ the zero-premises rule $DT$ and the *Markov Rule* below:

$$\frac{}{\exists xA(x) \vee \forall x(A(x) \to B \vee \neg B)}\ \mathrm{DT} \qquad \frac{\begin{array}{cc}\Gamma & \Gamma \\ \vdots\ {\scriptstyle \pi_1} & \vdots\ {\scriptstyle \pi_2} \\ \neg\neg\exists xA(x) & \forall x(A(x) \vee \neg A(x))\end{array}}{\exists xA(x)}\ \mathrm{Mk}$$

Now, let us use $\mathrm{RHA}^{++}$ to denote the union of the generalized rules CUT and SUBST, of the generalized rules ID, SUM, PROD described above and of the generalized rules

$$\begin{aligned}
&\mathrm{RDT}_1: \quad \vdash \exists xA(x) \in \mathrm{RDT}_1(\vdash A(t); \vdash \exists xA(x) \vee \forall x(A(x) \to B \vee \neg B)) \\
&\mathrm{RDT}_2: \quad \vdash \forall x(A(x) \to B \vee \neg B) \in \mathrm{RDT}_2(\vdash \exists xA(x) \vee \forall x(A(x) \to B \vee \neg B)) \\
&\mathrm{RDT}_3: \quad \vdash A(x) \to B \vee \neg B \in \mathrm{RDT}_3(\vdash \exists xA(x) \vee \forall x(A(x) \to B \vee \neg B))
\end{aligned}$$

It is easy to check that $\mathrm{RHA}^{++}$ is an e-rule for $\mathscr{ND}_{\mathbf{PA}}$. Let us use $\mathbb{ID}_{\mathbf{HA}^{++}}([\Pi])$ to denote the abstract calculus $\mathbb{ID}(\mathrm{RHA}^{++}, \mathrm{Seq}([\Pi]))$. The proof of uniform semiconstructivity of $\mathscr{ND}_{\mathbf{HA}^{++}}$ in $\mathscr{ND}_{\mathbf{PA}}$ follows the line of the proof given for $\mathscr{ND}_{\mathbf{HA}^{+}}$ but using the following notion of closed evaluation. Let $\Pi$ be a set of proofs on $\mathscr{L}_{\mathscr{A}}$ and let $A$ be a wff in the language $\mathscr{L}_{\mathscr{A}}$. *$A$ is evaluated in* $\Pi$ iff the following conditions hold:

1 There is a proof $\pi : \vdash A \in \Pi$.
2 For every closed instance $\theta A$ of $A$, one of the following conditions holds:
   (a) $\theta A$ is atomic or negated;
   (b) $\theta A \equiv B \wedge C$, and both $B$ and $C$ are evaluated in $\Pi$;
   (c) $\theta A \equiv B \vee C$, and either $B$ is evaluated in $\Pi$ or $C$ is evaluated in $\Pi$;
   (d) $\theta A \equiv B \to C$, and either $B$ is not evaluated in $\Pi$ or $C$ is evaluated in $\Pi$;
   (e) $\theta A \equiv \exists xB(x)$, and $B(t/x)$ is evaluated in $\Pi$ for some closed term $t$ of $\mathscr{L}_{\mathscr{A}}$;
   (f) $\theta A \equiv \forall xB(x)$, and, for every closed term $t$ of $\mathscr{L}_{\mathscr{A}}$, $B(t/x)$ is evaluated in $\Pi$.

A set $\Gamma$ of wff's is evaluated in a set of proofs $\Pi$ if every wff $A \in \Gamma$ is evaluated in $\Pi$. Hence the main lemma is as follows.

**Lemma 4.4.** Let $\Pi$ be any recursive set of proofs of $\mathscr{ND}_{\mathbf{HA}^{++}}$. For any proof $\pi : \Gamma \vdash H$ belonging to the closure under substitution of $[\Pi]$, if $\Gamma$ is evaluated in $\mathbb{ID}_{\mathbf{HA}^{++}}([\Pi])$, then $H$ is evaluated in $\mathbb{ID}_{\mathbf{HA}^{++}}([\Pi])$.

From the previous lemma, $\mathrm{Theo}([\Pi])$ is semiconstructive in $\mathrm{Theo}(\mathbb{ID}_{\mathbf{HA}^{++}}([\Pi]))$ and, since $\mathrm{RHA}^{++}$ is an e-rule for $\mathscr{ND}_{\mathbf{PA}}$, we get the following theorem.

**Theorem 4.5.** $\mathscr{ND}_{\mathbf{HA}^{++}}$ is a uniformly semiconstructive calculus in $\mathscr{ND}_{\mathbf{PA}}$.

Hence $\mathbf{HA}^{++} = \mathrm{Theo}(\mathscr{ND}_{\mathbf{HA}^{++}})$ is a uniformly semiconstructive **HA**-system.

We should point out that the well-known *Scott Principle* $(\mathrm{St}) = ((\neg\neg A \to A) \to A \vee \neg A) \to \neg A \vee \neg\neg A$ (Rose 1953) is derivable from (DT). On the other hand, the addition of both (St) and $(\mathrm{KP}_{\exists})$ to **HA** gives rise to an **HA**-system that is not semiconstructive (Ferrari *et al.* 1999b), which implies that there is no semiconstructive **HA**-system that contains both the semiconstructive **HA**-systems $\mathbf{HA}^{+}$ and $\mathbf{HA}^{++}$ (in particular, $\mathbf{HA}^{+} \nsubseteq \mathbf{HA}^{++}$ and $\mathbf{HA}^{++} \nsubseteq \mathbf{HA}^{+}$). We remark that we can add to $\mathscr{ND}_{\mathbf{HA}^{++}}$ the rule Kur without affecting its uniform semiconstructivity (and without extending the generalized rule $\mathrm{RHA}^{++}$). However, we can prove that $\mathbf{HA}^{++}$ cannot be extended into a recursively enumerable and constructive **T**-system with $\mathbf{HA} \subseteq \mathbf{T}$.

**Theorem 4.6.** There exists no consistent and recursively axiomatizable constructive **T**-system **S** such that $\mathbf{HA} \subseteq \mathbf{T}$ and $\mathbf{HA}^{++} \subseteq \mathbf{S}$.

We conclude by remarking that the extraction mechanism described in this paper is rather general. It can be applied to a wide family of **T**-systems including theories with isoinitial model (Miglioli *et al.* 1994) and logical and mathematical principles of interest in the framework of program synthesis and formal verification (Thompson 1991; Avellone *et al.* 1999). Finally, we would like to remark that the notion of uniformly semiconstructive formal system does not collapse into the notion of semiconstructive formal system; in fact, in Ferrari *et al.* (1999b) the authors exhibit a formal system obtained by adding to Intuitionistic Arithmetic a single axiom schema that is semiconstructive but is not uniformly semiconstructive.

## References

Avellone, A., Ferrari, M. and Miglioli, P. (1999) Synthesis of programs in abstract data types. In: 8th International Workshop on Logic-based Program Synthesis and Transformation. *Springer-Verlag Lecture Notes in Computer Science* **1559** 81–100.

Benini, M. (1999) *Verification and Analysis of Programs in a Constructive Environment*, Ph. D. thesis, Dip. di Scienze dell'Informazione, Univ. di Milano, Italy.

Ferrari, M. (1997) *Strongly Constructive Formal Systems*, Ph. D. thesis, Dip. di Scienze dell'Informazione, Univ. di Milano, Italy.

Ferrari, M., Fiorentini, C. and Miglioli, P. (1999a) Goal oriented information extraction in uniformly constructive calculi. In: *Proceedings of WAIT'99: Workshop Argentino de Informática Teórica* 51–63.

Ferrari, M., Fiorentini, C. and Miglioli, P. (2000) Extracting information from intermediate T-systems. Technical Report 252-00, Dip. Scienze dell'Informazione, Univ. di Milano, Italy.

Ferrari, M., Miglioli, P. and Ornaghi, M. (1999b) On uniformly constructive and semiconstructive formal systems. Submitted to *Annals of Pure and Applied Logic*.

Kleene, S. (1945) On the interpretation of intuitionistic number theory. *Journal of Symbolic Logic* **10** (4) 109–124.

Miglioli, P., Moscato, U. and Ornaghi, M. (1989) Semi-constructive formal systems and axiomatization of abstract data types. In: Diaz, J. and Orejas, F. (eds.) TAPSOFT'89. *Springer-Verlag Lecture Notes in Computer Science* 337–351.

Miglioli, P., Moscato, U. and Ornaghi, M. (1994) Abstract parametric classes and abstract data types defined by classical and constructive logical methods. *Journal of Symbolic Computation* **18** 41–81.

Miglioli, P. and Ornaghi, M. (1981) A logically justified model of computation I & II. *Fundamenta Informaticae* IV (1, 2) 151–172, 277–341.

Ono, H. (1972) Some results on the intermediate logics. *Publications of the Research Institute for Mathematical Sciences, Kyoto University* **8** 117–130.

Rose, G. (1953) Propositional calculus and realizability. *Trans. Amer. Math. Soc.* **75** 1–18.

Thompson, S. (1991) *Type Theory and Functional Programming*, Addison-Wesley.

Troelstra, A. (ed.) (1973) Metamathematical Investigation of Intuitionistic Arithmetic and Analysis. *Springer-Verlag Lecture Notes in Mathematics* **344**.