Formalizing and Proving Semantic Relations between Specifications by Reflection*

Manuel Clavel, Narciso Martí-Oliet, and Miguel Palomino

Departamento de Sistemas Informáticos y Programación
Universidad Complutense de Madrid, Spain
{clavel, narciso, miguelpt}@sip.ucm.es

Abstract. This work contains both a theoretical development and a novel application of ideas introduced in [1] for using reflection in formal metareasoning. From the theoretical side, we extend the metareasoning principles proposed in [1] to cover the case of metatheorems about equational theories which are unrelated by the inclusion relation. From the practical side, we apply the newly introduced metareasoning principles to formalize and prove semantic relations between equational theories used in formal specification.

1 Introduction

Intuitively, a *reflective* logic is a logic in which important aspects of its metalogic can be represented at the object level in a consistent way, so that the object-level representations correctly simulate the relevant metalogical aspects. More concretely, a logic is reflective when there exists a theory —that we call *universal*— in which we can represent and reason about all finitely presentable theories in the logic, including the universal theory itself [8, 3]. As a consequence, in a reflective logic, metatheorems involving families of theories can be represented and logically proved as theorems about its universal theory. Of course, one of the advantages of formal metareasoning based on reflection is that it can be carried out using already existing logical reasoning tools.

The use of reflection for formal metareasoning was first proposed in [1], both abstractly and concretely. Abstractly, it proposes a set of requirements for a logic to be used as a reflective metalogical framework. Concretely, it presents membership equational logic [12] as a particular logic that satisfies those requirements. In addition, it provides metareasoning principles to logically prove metatheorems about families of membership equational theories as theorems about its universal theory [9].

This work is both a development and an application of the reflective methodology proposed in [1] for formal metareasoning using membership equational logic. First, we extend the metareasoning principles introduced in [1]. In particular, while [1] only considered metatheorems about membership equational

* Research supported by Spanish MCYT Projects MELODIAS TIC2002-01167 and MIDAS TIC2003-01000, and CICYT Project AMEVA TIC2000-0701-C02-01.

theories which are related by the inclusion relation, our reflective methodology can also deal with metatheorems about theories which are unrelated with respect to inclusion. Thus, our extension increases significantly the applicability of the reflective methodology proposed in [1], as we show with the following case study. As is well-known, equational specifications can be related in different ways, and these relations can be informally formulated as metalogical statements of equational logic. The semantic relations between different equational specifications are in fact key conceptual tools in the stepwise specification methodology, and different techniques and criteria have been proposed to metalogically prove them [10]. We show that some of these semantic relations can be formalized as theorems about the universal theory of membership equational logic and that they can be logically proved in a way that mirrors their corresponding proofs at the metalogical level.

Organization The paper is organized as follows. First, in Sect. 2 we introduce membership equational logic; the content of this section is standard material borrowed from other papers. Then, in Sect. 3 we formulate some semantic relations between membership equational specifications as metalogical statements, and in Sect. 4 we introduce metareasoning principles for metalogically proving them. Finally, in Sects. 5, 6, and 7 we present our reflective framework, and we put it to work. In particular, we show how a whole class of metalogical statements, that contains those in Sects. 3 and 4, can be represented and logically proved, using reflection, in membership equational logic; we include in an appendix a detailed example of this.

2 Membership Equational Logic

Membership equational logic is an expressive version of equational logic. A full account of the syntax and semantics of membership equational logic can be found in [2, 12]. Here we define the basic notions needed in this paper.

A *signature* in membership equational logic is a triple $\Omega = (K, \Sigma, S)$ with K a set of *kinds*, Σ a K-kinded signature $\Sigma = \{\Sigma_{k_1 \ldots k_n, k}\}_{(k_1 \ldots k_n, k) \in K^* \times K}$, and $S = \{S_k\}_{k \in K}$ a pairwise disjoint K-kinded family of sets. We call S_k the set of *sorts* of kind k. The pair (K, Σ) is what is usually called a many-sorted signature of function symbols; however we call the elements of K *kinds* because each kind k now has a set S_k of associated *sorts*, which in the models will be interpreted as subsets of the carrier for the kind.

The atomic formulae of membership equational logic are either *equations* $t = t'$, where t and t' are Σ-terms of the same kind, or *membership assertions* of the form $t : s$, where the term t has kind k and $s \in S_k$. Sentences are Horn clauses on these atomic formulae, i.e., sentences of the form

$$\forall (x_1, \ldots, x_m).\, A_1 \wedge \ldots \wedge A_n \Longrightarrow A_0\,,$$

where each A_i is either an equation or a membership assertion, and each x_j is a K-kinded variable. A theory in membership equational logic is a pair (Ω, E),

where E is a finite set of sentences in membership equational logic over the signature Ω. We write $(\Omega, E) \vdash \phi$ to denote that (Ω, E) entails the sentence ϕ.

We employ standard semantics concepts from many-sorted logic. Given a signature $\Omega = (K, \Sigma, S)$, an *Ω-algebra* is a many-kinded Σ-algebra (that is, a K-indexed-set $A = \{A_k\}_{k \in K}$ together with a collection of appropriately kinded functions interpreting the function symbols in Σ) and an assignment that associates to each sort $s \in S_k$ a subset $A_s \subseteq A_k$. An algebra A and a valuation σ, assigning to variables of kind k values in A_k, satisfy an equation $t = t'$ iff $\sigma(t) = \sigma(t')$. We write $A, \sigma \models t = t'$ to denote such a satisfaction. Similarly, $A, \sigma \models t\!:\!s$ holds iff $\sigma(t) \in A_s$.

Note that an Ω-algebra is a K-kinded first-order model with function symbols Σ and a kinded alphabet of unary predicates $\{S_k\}_{k \in K}$. We can then extend the satisfaction relation to Horn and first-order formulae ϕ over the atomic formulae in the standard way. We write $A \models \phi$ when the formula ϕ is satisfied for all valuations σ, and then say that A is a model of ϕ. As usual, we write $(\Omega, E) \models \phi$ when all the models of the set E of sentences are also models of ϕ. As expected, the rules of inference for membership equational logic are sound and complete.

Theories in membership equational logic have initial models. This provides the basis for reasoning by induction. In the initial model of a membership equational theory, sorts are interpreted as the smallest sets satisfying the axioms in the theory, and equality is interpreted as the smallest congruence satisfying those axioms. Given a theory (Ω, E), we denote its initial model by $T_{\Omega/E}$. In particular, when $E = \emptyset$ we obtain the term algebra T_Ω, and for X a K-kinded set of variables the free algebra $T_\Omega(X)$. We write $(\Omega, E) \trianglerighteq \phi$ to denote that the initial model of the membership equational theory (Ω, E) is also a model of ϕ, that is, that the satisfaction relation $T_{\Omega/E} \models \phi$ holds.

3 Semantic Relations between Specifications

The formalization and proof of certain semantic relations between equational specifications are important aspects of the algebraic specification methodology. In this regard, a classical notion is that of *enrichment*, which is a key conceptual tool in the stepwise specification methodology [10, 11]. We consider the following definition of the enrichment relation between membership equational specifications.

Definition 1. *Let $R = (\Omega, E)$ and $R' = (\Omega', E')$ be specifications, with $\Omega = (K, \Sigma, S)$ and $\Omega' = (K', \Sigma', S')$, such that $R \subseteq R'$ componentwise. Let k be a kind in K, and let s be a sort in S_k. Then R' is an* s-enrichment *of R if and only if:*

1-a. $\forall t \in T_{\Omega'}.\, R' \vdash t\!:\!s \Longrightarrow \exists t' \in T_\Omega.\, R \vdash t'\!:\!s \wedge R' \vdash t = t'$
1-b. $\forall t, t' \in T_\Omega.\, R \vdash t\!:\!s \wedge R \vdash t'\!:\!s \wedge R' \vdash t = t' \Longrightarrow R \vdash t = t'$.

Note that our definition is slightly different from that in [10] —(1-a) and (1-b) correspond, respectively, to their notions of *complete* and *consistent extensions*—

since we define the enrichment relation relative to a particular sort. The idea captured by our definition is that each ground term in the specification R' having the sort s can be proved equal to a ground term of the specification R having the sort s, and also that R' does not impose new equalities on ground terms of sort s of the specification R. These properties correspond, respectively, to the *no junk* and *no confusion* properties in Burstall and Goguen's terminology.

The enrichment relation assumes an inclusion between the given specifications. There are other semantic relations, however, that do not require such an inclusion. Consider, for example, the specifications INT_1 and INT_2 below. They are presented using Maude syntax [5, 6], where operators, variables, membership axioms, and equations are introduced, respectively, with the keywords `op`, `var`, `mb` (or `cmb` for the conditional case), and `eq`. The Maude system implements membership equational logic (and rewriting logic) and can infer kind information automatically; however, for increased clarity, we have explicitly named kinds, with their associated sort lists inside square brackets following the kind's name. The specifications INT_1 and INT_2 are clearly related since both specify the integer numbers —and, in that sense, they are *interchangeable*—, but neither INT_1 is included in INT_2, nor INT_2 in INT_1.

```
fmod INT1 is
kind Num[Neg, Nat, Int] .
op 0 : -> Num .
op s : Num -> Num .
op p : Num -> Num .
var N : Num .
--- Nonpositive numbers
mb 0 : Neg .
cmb p(N) : Neg if N : Neg .
--- Natural numbers
mb 0 : Nat .
cmb s(N) : Nat if N : Nat .

--- Integers
cmb N : Int if N : Neg .
cmb N : Int if N : Nat .
endfm
```

```
fmod INT2 is
kind Num[Int] .
op 0 : -> Num .
op s : Num -> Num .
op p : Num -> Num .
var N : Num .
--- Integers
mb 0 : Int .
cmb s(N) : Int if N : Int .
cmb p(N) : Int if N : Int .
eq p(s(N)) = N .
eq s(p(N)) = N .
endfm
```

We propose the following definition for this particular relation between membership equational specifications. For the sake of simplicity, we restrict our definition to specifications with a common set of kinds.

Definition 2. *Let $R = (\Omega, E)$ and $R' = (\Omega', E')$ be specifications, with $\Omega = (K, \Sigma, S)$ and $\Omega' = (K, \Sigma', S')$. Let k be a kind in K, and let s be a sort in $S_k \cap S'_k$. Then R and R' are* s-interchangeable *if and only if:*

2-a. $\forall t \in T_\Omega.\, R \vdash t : s \Longrightarrow \exists t' \in T_{\Omega'}.\, R' \vdash t' : s \wedge R \vdash t = t'$
2-b. $\forall t, t' \in T_{\Omega'}.\, R' \vdash t : s \wedge R' \vdash t' : s \wedge R \vdash t = t' \Longrightarrow R' \vdash t = t'$
2-c. $\forall t \in T_{\Omega'}.\, R' \vdash t : s \Longrightarrow \exists t' \in T_\Omega.\, R \vdash t' : s \wedge R' \vdash t = t'$

2-d. $\forall t, t' \in T_\Omega.\, R \vdash t\!:\!s \wedge R \vdash t'\!:\!s \wedge R' \vdash t = t' \Longrightarrow R \vdash t = t'$.

The idea captured by the above definition is that each ground term in the specification R' (resp. R) having the sort s can be proved equal to a ground term of the specification R (resp. R') having the sort s, and also that R' (resp. R) does not impose new equalities on ground terms of sort s of the specification R (resp. R').

Now, note that to prove properties (1-b), (2-b), and (2-d) we need, in general, to examine the form of the axioms in R and R'. But to prove properties (1-a), (2-a), and (2-c) we can use inductive techniques. In fact, an inductive reasoning principle is proposed in [2] to logically prove property (1-a). However, the lack of an inclusion between R and R' invalidates the use of this principle for proving properties (2-a) and (2-c). We will propose in Sect. 4 an inductive reasoning principle (ind^+) to metalogically prove these properties, and we will show in Sect. 7 how this principle can be transformed, using reflection, into an inductive reasoning principle ($\overline{ind^+}$) to logically prove them.

4 An Inductive Principle for Metalogically Proving Semantic Relations

In order to provide a simpler and more compact formulation, and soundness proof, of an inductive principle (ind^+) for *metalogically* proving semantic relations between equational specifications, we begin by extending the definitions of terms, atomic formulae, and entailment relation for membership equational logic. Basically, these extensions allow us to metareason on equivalence classes of terms, instead than on concrete terms, which is essential for metareasoning about families of theories which are unrelated with respect to inclusion. However, this change of logical framework is only transitory. We will show in Sect. 7 how the inductive principle (ind^+) can be transformed, using reflection, into an inductive principle ($\overline{ind^+}$) for *logically* proving, in standard membership equational logic, semantic relations between equational specifications. Of course, since our final goal is to provide principles for carrying out formal metareasoning, we are interested in ($\overline{ind^+}$) rather than in (ind^+), but we introduce the latter as a technical device to simplify the presentation and proof of the former.

In what follows, let $\mathcal{CR}$ be the class of finite multisets of finitely presentable theories with a common, nonempty set of kinds $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i \in [1..p]}$, with each $\Omega_i = (K, \Sigma_i, S_i)$. We consider multisets instead of lists or sets for technical reasons: it simplifies our definition of the inductive principles (ind^+).

Definition 3. *Given* $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i \in [1..p]} \in \mathcal{CR}$*, with each* $\Omega_i = (K, \Sigma_i, S_i)$*, we define the set* $T^{\mathcal{R}}_{\Omega_i}(X)$ *of* $(\Omega_i, \mathcal{R})$*-terms with* K*-kinded variables in* X *as follows:*

- $c \in (T^{\mathcal{R}}_{\Omega_i}(X))_k$ *iff* $c \in (\Sigma_i)_{\lambda,k}$*,* $k \in K$*, where* λ *denotes the empty sequence of kinds;*
- $x \in (T^{\mathcal{R}}_{\Omega_i}(X))_k$ *iff* $x \in X_k$*,* $k \in K$*;*

– $f(t_1, \ldots, t_n) \in (T^{\mathcal{R}}_{\Omega_i}(X))_k$ *iff* $f \in (\Sigma_i)_{k_1 \ldots k_n, k}$, *and* $t_j \in (T^{\mathcal{R}}_{\Omega_i}(X))_{k_j}$, *for* $j = 1, \ldots, n$,
– $[t]_{R_j} \in (T^{\mathcal{R}}_{\Omega_i}(X))_k$ *iff* $R_j \in \mathcal{R}$ *and* $t \in (T^{\mathcal{R}}_{\Omega_j}(X))_k$.

As we will formalize in Def. 5 below the intended meaning of the term $[t]_{R_j}$, in the particular case that $t \in T_{\Omega_j}$, is the equivalence class of the terms provably equal to t in the theory R_j.

Definition 4. *Given* $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i \in [1..p]} \in \mathcal{CR}$, *with each* $\Omega_i = (K, \Sigma_i, S_i)$, *an atomic* $(\Omega_i, \mathcal{R})$*-formula is either an equation* $t = t'$, *where* t *and* t' *are* $(\Omega_i, \mathcal{R})$*-terms of the same kind, or a membership assertion of the form* $t\!:\!s$, *where the* $(\Omega_i, \mathcal{R})$*-term* t *has kind* k *and* $s \in (S_i)_k$.

Definition 5. *Given* $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i \in [1..p]} \in \mathcal{CR}$, *with each* $\Omega_i = (K, \Sigma_i, S_i)$, *for all theories* $R_i \in \mathcal{R}$ *and atomic* $(\Omega_i, \mathcal{R})$*-formulae* ϕ, *we recursively define the entailment relation* $\vdash^{\mathcal{R}}$ *as follows:*

– *if there is a position* p *in* ϕ *(for an appropriate definition of positions in atomic formulae), and a term* $t \in (T_{\Omega_j})_k$, *with* $R_j \in \mathcal{R}$, *such that* $[t]_{R_j}$ *occupies position* p *in* ϕ, *then*

$$R_i \vdash^{\mathcal{R}} \phi \text{ iff } \exists t' \in (T_{\Omega_i})_k \cap (T_{\Omega_j})_k . \, (R_i \vdash^{\mathcal{R}} \phi[t']_p \wedge R_j \vdash t = t') \,,$$

where $\phi[t']_p$ *is the replacement operation of the term* t' *inside the atomic formula* ϕ *at position* p;
– *otherwise,* $R_i \vdash^{\mathcal{R}} \phi$ *iff* $R_i \vdash \phi$.

According to this definition, a theory R_i entails an atomic $(\Omega_i, \mathcal{R})$-formula ϕ if ϕ can be proved in R_i after recursively replacing all occurrences of terms $[t]_{R_j}$, such that $t \in T_{\Omega_j}$, with appropriate ground terms in the corresponding equivalence classes.

Remark 1. Given $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i \in [1..p]} \in \mathcal{CR}$, with each $\Omega_i = (K, \Sigma_i, S_i)$, for all theories $R_i, R_j \in \mathcal{R}$, atomic $(\Omega_i, \mathcal{R})$-formulae $\phi(x)$, with free variable x of kind k, and terms $t, t' \in (T_{\Omega_i})_k \cap (T_{\Omega_j})_k$, the following statements hold:

– if $R_j \vdash t = t'$, then $R_i \vdash^{\mathcal{R}} \phi([t]_{R_j})$ iff $R_i \vdash^{\mathcal{R}} \phi([t']_{R_j})$;
– $R_i \vdash^{\mathcal{R}} \phi(t)$ iff $R_i \vdash^{\mathcal{R}} \phi([t]_{R_i})$;
– if $R_i \vdash^{\mathcal{R}} \phi(t)$ then $R_i \vdash^{\mathcal{R}} \phi([t]_{R_j})$;
– if $E_j \subseteq E_i$, then $R_i \vdash^{\mathcal{R}} \phi(t)$ iff $R_i \vdash^{\mathcal{R}} \phi([t]_{R_j})$; and
– if E_j does not include any equations, then $R_i \vdash^{\mathcal{R}} \phi(t)$ iff $R_i \vdash^{\mathcal{R}} \phi([t]_{R_j})$.

For example, using these extended definitions of terms, atomic formulae, and entailment relation for membership equational logic, we can express, in a simple and compact way, property (2-c) with respect to INT_2 and INT_1 by the following metalogical statement:

$$\forall t \in (T_{INT_2})_{Num} . (INT_2 \vdash t\!:\!Int \Longrightarrow INT_1 \vdash^{\mathcal{I}} [t]_{INT_2}\!:\!Int) \,, \qquad (1)$$

where $\mathcal{I}$ is the multiset $\{INT_1, INT_2\}$.

We are now ready to prove in Prop. 1 below an inductive principle (ind^+) for metalogically proving metatheorems about finite multisets of theories $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i\in[1..p]}$ in $\mathcal{CR}$. Since this proposition is rather technical, we informally advance its content.

- The inductive principle (ind^+) can be applied to metalogical statements of the form: "for all terms t of a sort s in a membership equational theory R_i in $\mathcal{R}$, some property P holds." Here, P is a Boolean expression, $bexp(B_1, \ldots, B_p)$, whose propositional variables are instantiated with metalogical statements of the form: "an atomic $(\Omega_j, \mathcal{R})$-formula $\phi([t]_{R_i})$ holds in R_j," with respect to our extended definition of the entailment relation. For example, the metalogical statement (1) belongs to the class of metatheorems to which our inductive principle can be applied.
- The inductive cases generated by the inductive principle (ind^+) are directly derived from the inductive definition of the sort s in the membership equational theory R_i. Therefore, our inductive cases mirror the inductive cases generated by the usual structural induction principle for membership equational theories. For example, the three inductive cases generated by (ind^+) when applied to the metalogical statement (1) correspond to the three cases in the inductive definition of the sort *Int* in INT_2: namely, 0 is an *Int*; $s(n)$ is an *Int*, if n is an *Int*; and $p(n)$ is an *Int*, if n is an *Int*.

In what follows, given a term $u \in T^{\mathcal{R}}_{\Omega}(X)$, we denote by $u(x_1, \ldots, x_n)$, or just $u(\vec{x})$, the fact that the variables in u are in the set $\vec{x} = \{x_1, \ldots, x_n\} \subseteq X$. Thus, given a set $\{t_1, \ldots, t_n\}$ of *metavariables*, we denote by $u(\vec{t})$ the simultaneous replacement of x_i by t_i in u, for $i = 1, \ldots, n$. Similarly, given an atomic formula $\phi(\vec{x})$ with free variables in $\vec{x}$, we denote by $\phi(\vec{t})$ the simultaneous replacement of x_i by t_i in ϕ, for $i = 1, \ldots, n$.

Proposition 1. *Let $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i\in[1..p]}$ be a finite multiset of theories in $\mathcal{CR}$, with each $\Omega_i = (K, \Sigma_i, S_i)$. Let s be a sort in some $(S_e)_k$, $e \in [1..p]$ and $k \in K$, and let $C_{[R_e,s]} = \{C_1, \ldots, C_n\}$ be those sentences in E_e that specify s, i.e., those C_i of the form*

$$\forall(x_1, \ldots, x_{r_i}).\, A_1 \wedge \ldots \wedge A_{q_i} \Longrightarrow A_0\,, \tag{2}$$

where, for $1 \leq j \leq r_i$, x_j is of kind k_{i_j}, and for some term w of kind k, A_0 is $w{:}s$.

Then, for all finite multisets of atomic formulae, $\{\phi_l(x)\}_{l\in[1..p]}$, with each $\phi_l(x)$ an atomic $(\Omega_l, \mathcal{R})$-formula with free variable x of kind k, and Boolean expressions bexp, the following metalogical statement holds:

$$\begin{aligned} &\psi_1 \wedge \ldots \wedge \psi_n \\ &\Longrightarrow \forall t \in (T_{\Omega_e})_k.\, (R_e \vdash t{:}s \Longrightarrow bexp(R_1 \vdash^{\mathcal{R}} \phi_1([t]_{R_e}), \ldots, R_p \vdash^{\mathcal{R}} \phi_p([t]_{R_e})))\,, \end{aligned} \tag{3}$$

where, for $1 \leq i \leq n$ and C_i in E_e of the form (2), ψ_i is

$$\forall t_1 \in (T_{\Omega_e})_{k_{i_1}} \ldots \forall t_{r_i} \in (T_{\Omega_e})_{k_{i_{r_i}}}.\, [A_1]^\sharp \wedge \ldots \wedge [A_{q_i}]^\sharp \Longrightarrow [A_0]^\sharp$$

and, for $0 \leq j \leq q_i$,

$$[A_j]^\sharp \triangleq \begin{cases} \mathit{bexp}\left(R_1 \vdash^{\mathcal{R}} \phi_1([u(\vec{t})]_{R_e}), \ldots, R_p \vdash^{\mathcal{R}} \phi_p([u(\vec{t})]_{R_e})\right) & \text{if } A_j = u : s \\ R_e \vdash A_j(\vec{t}) & \text{otherwise.} \end{cases}$$

The metalogical statement (3) *introduces an inductive metareasoning principle* (ind^+)*, where each* ψ_i *corresponds to an inductive case and the top line in the definition of* $[A_j]^\sharp$ *provides the corresponding induction hypotheses.*

Proof (soundness). Assume that $\psi_1 \wedge \cdots \wedge \psi_n$ holds. We must prove that

$$\forall t \in (T_{\Omega_e})_k . (R_e \vdash t : s \Longrightarrow \mathit{bexp}(R_1 \vdash^{\mathcal{R}} \phi_1([t]_{R_e}), \ldots, R_p \vdash^{\mathcal{R}} \phi_p([t]_{R_e})))$$

also holds. Let $t \in (T_{\Omega_e})_k$ be a term such that $R_e \vdash t : s$; we proceed by structural induction on this derivation. If $R_e \vdash t : s$, then there exists a sentence C_i in E_e of the form $\forall(x_1, \ldots, x_{r_i}). A_1 \wedge \ldots \wedge A_{q_i} \Longrightarrow A_0$, where, for $1 \leq j \leq r_i$, x_j is of kind k_{i_j}, and for some term w of kind k, A_0 is $w : s$, and a substitution $\sigma : \{x_1, \ldots, x_{r_i}\} \longrightarrow T_{\Omega_e}$, such that

- $R_e \vdash t = \sigma(w)$, and
- $R_e \vdash \sigma(A_j)$, for $1 \leq j \leq q_i$.

In this case, we must prove that $\mathit{bexp}(R_1 \vdash^{\mathcal{R}} \phi_1([t]_{R_e}), \ldots, R_p \vdash^{\mathcal{R}} \phi_p([t]_{R_e}))$ holds, under the inductive hypothesis that, for $1 \leq j \leq q_i$, if $A_j = u_j : s$, then $\mathit{bexp}\left(R_1 \vdash^{\mathcal{R}} \phi_1([\sigma(u_j)]_{R_e}), \ldots, R_p \vdash^{\mathcal{R}} \phi_p([\sigma(u_j)]_{R_e})\right)$ holds. Since, by assumption, ψ_i holds, then it also holds $[A_1]^\sharp_\sigma \wedge \ldots \wedge [A_{q_i}]^\sharp_\sigma \Longrightarrow [A_0]^\sharp_\sigma$, where, for $0 \leq j \leq q_i$,

$$[A_j]^\sharp_\sigma \triangleq \begin{cases} \mathit{bexp}\left(R_1 \vdash^{\mathcal{R}} \phi_1([\sigma(u_j)]_{R_e}), \ldots, R_p \vdash^{\mathcal{R}} \phi_p([\sigma(u_j)]_{R_e})\right) & \text{if } A_j = u_j : s \\ R_e \vdash \sigma(A_j) & \text{otherwise.} \end{cases}$$

Note then that, for $1 \leq j \leq q_i$,

- If $A_j = (u_j : s)$, then $[A_j]^\sharp_\sigma$ holds by induction hypothesis.
- If $A_j \neq (u_j : s)$, then $[A_j]^\sharp_\sigma$ holds by assumption.

Hence, $[A_0]^\sharp_\sigma$, that is, $\mathit{bexp}(R_1 \vdash^{\mathcal{R}} \phi_1([\sigma(w)]_{R_e}), \ldots, R_p \vdash^{\mathcal{R}} \phi_p([\sigma(w)]_{R_e}))$, also holds. Finally, since $R_e \vdash t = \sigma(w)$, by Rem. 1, we have that $\mathit{bexp}(R_1 \vdash^{\mathcal{R}} \phi_1([t]_{R_e}), \ldots, R_p \vdash^{\mathcal{R}} \phi_p([t]_{R_e}))$ as required. □

As a final remark, note that a case analysis metareasoning principle ($case^+$) can be introduced in a way entirely similar to (ind^+), except of course for the definition of $[A_j]^\sharp$, that will be as follows (see [7] for more details):

$$[A_j]^\sharp \triangleq \begin{cases} \mathit{bexp}\left(R_1 \vdash^{\mathcal{R}} \phi_1([u(\vec{t})]_{R_e}), \ldots, R_p \vdash^{\mathcal{R}} \phi_p([u(\vec{t})]_{R_e})\right) & \text{if } j = 0 \\ R_e \vdash A_j(\vec{t}) & \text{otherwise.} \end{cases}$$

5 Reflection in Membership Equational Logic

A logic is reflective when there exists a *universal* theory in which we can represent and reason about all finitely presentable theories in the logic, including the universal theory itself [8, 3]. A universal theory `MB-META` for membership equational logic was introduced in [9], along with a representation function $\overline{(\_ \vdash \_)}$ that encodes pairs, consisting of a finitely presentable membership equational theory with nonempty kinds and a sentence in it, as sentences in `MB-META`. The signature of `MB-META` contains constructors to represent operators, variables, terms, kinds, sorts, signatures, axioms, and theories. In particular, the signature of `MB-META` includes the sorts `Op`, `Var`, `Term`, `TermList`, `Kind`, `Sort`, and `Theory` for terms representing, respectively, operators, variables, terms, lists of terms, kinds, sorts, and theories. In addition, it contains three Boolean operators

```
op _::_in_ : [Term] [Kind] [Theory] -> [Bool] .
op _:_in_ : [Term] [Sort] [Theory] -> [Bool] .
op _=_in_ : [Term] [Term] [Theory] -> [Bool] .
```

to represent, respectively, that a term is a ground term of a given kind in a membership equational theory, and that a membership assertion or an equation holds in a membership equational theory. Note that here, and in what follows, we use Maude's convention for naming kinds: kinds are not named but denoted using the name of their sorts enclosed in square brackets.

The representation function $\overline{(\_ \vdash \_)}$ is defined in [9] as follows: for all finitely presentable membership equational theories with nonempty kinds R and atomic formulae ϕ over the signature of R,

$$\overline{R \vdash \phi} \triangleq \begin{cases} (\overline{t} : \overline{s} \texttt{ in } \overline{R}) = \texttt{true} \text{ if } \phi = (t\!:\!s) \\ (\overline{t} = \overline{t'} \texttt{ in } \overline{R}) = \texttt{true} \text{ if } \phi = (t = t') \,, \end{cases}$$

where $\overline{(\_)}$ is a representation function defined recursively over theories, signatures, axioms, and so on. Under this representation function, a term t is represented in `MB-META` by a ground term $\overline{t}$ of sort `Term`, a kind k is represented by a ground term $\overline{k}$ of sort `Kind`, a sort s is represented by a ground term $\overline{s}$ of sort `Sort`, and a theory R is represented by a ground term $\overline{R}$ of sort `Theory`. In particular, to represent terms the signature of `MB-META` contains the constructors

```
op _[_] : [Op] [TermList] -> [Term] .
op nil : -> [TermList] .
op _,_ : [TermList] [TermList] -> [TermList] .
```

and the representation function $\overline{(\_)}$ is defined as follows:

$$\overline{t} \triangleq \begin{cases} \overline{c} & \text{if } t = c \text{ is a constant} \\ \overline{x} & \text{if } t = x \text{ is a variable} \\ \overline{f}\,[\overline{t_1}, \ldots, \overline{t_n}] & \text{if } t = f(t_1, \ldots, t_n). \end{cases}$$

For example, the term $s(0)$ of kind *Num* is represented in `MB-META` as the term $\overline{s}\,[\overline{0}]$ of sort `Term`.

The following propositions state the main properties of MB-META as a universal theory [9]:

Proposition 2. *For all finitely presentable membership equational theories with nonempty kinds $R = (\Omega, E)$, with $\Omega = (K, \Sigma, S)$, terms t in T_Ω, and kinds $k \in K$,*

$$t \in (T_\Omega)_k \Longleftrightarrow \texttt{MB-META} \vdash (\overline{t} \texttt{ :: } \overline{k} \texttt{ in } \overline{R}) = \texttt{true}\,.$$

Proposition 3. *For all finitely presentable membership equational theories with nonempty kinds $R = (\Omega, E)$, with $\Omega = (K, \Sigma, S)$, kinds $k \in K$, and ground terms u of the kind* [Term]*, if*

$$\texttt{MB-META} \vdash (u \texttt{ :: } \overline{k} \texttt{ in } \overline{R}) = \texttt{true}\,,$$

then there is a term $t \in (T_\Omega)_k$ such that $\overline{t} = u$.

Proposition 4. *For all finitely presentable membership equational theories with nonempty kinds $R = (\Omega, E)$, with $\Omega = (K, \Sigma, S)$, terms t in $(T_\Omega)_k$ and sorts s in S_k,*

$$R \vdash t : s \iff \texttt{MB-META} \vdash (\overline{t} \texttt{ : } \overline{s} \texttt{ in } \overline{R}) = \texttt{true}.$$

Similarly, for all terms t, t' in $(T_\Omega)_k$,

$$R \vdash t = t' \iff \texttt{MB-META} \vdash (\overline{t} \texttt{ = } \overline{t'} \texttt{ in } \overline{R}) = \texttt{true}\,.$$

For example,

$$\texttt{MB-META} \vdash (\overline{\texttt{p(s(p(0)))}} \texttt{ : } \overline{\texttt{Int}} \texttt{ in } \overline{\texttt{INT2}}) = \texttt{true}\,,$$

but

$$\texttt{MB-META} \nvdash (\overline{\texttt{p(s(p(0)))}} \texttt{ : } \overline{\texttt{Int}} \texttt{ in } \overline{\texttt{INT1}}) = \texttt{true}\,.$$

6 Reflection in Extended Membership Equational Logic

To represent and reason about our extended definition of entailment relation, we define a new theory $\texttt{MB-META}^{=}$ that extends the universal theory MB-META with a binary operator

```
op _in_ : [Term] [Theory] -> [Term] .
ceq (t' in R) = (t'' in R) if (t' = t'' in R) = true .
```

to represent the equivalence class of a term in a membership equational theory.

Proposition 5. *For all finitely presentable membership equational theories with nonempty kinds $R = (\Omega, E)$, with $\Omega = (K, \Sigma, S)$, and terms t, t' in $(T_\Omega)_k$, $k \in K$,*

$$R \vdash t = t' \iff \texttt{MB-META}^{=} \vdash (\overline{t} \texttt{ in } \overline{R}) = (\overline{t'} \texttt{ in } \overline{R})\,.$$

Using this operator, we can now define a representation function $\overline{(\_)}$ for terms in the extended class, which satisfies the expected property, as shown in Prop. 6 below. Let $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i\in[1..p]}$ be a finite multiset of theories in $\mathcal{CR}$. Then, for all terms $t \in T^{\mathcal{R}}_{\Omega}(X)$,

$$\overline{t} \triangleq \begin{cases} \overline{c} & \text{if } t = c \text{ is a constant} \\ \overline{x} & \text{if } t = x \text{ is a variable} \\ \overline{f}\,\texttt{[}\overline{t_1}\texttt{, } \ldots \texttt{,}\overline{t_n}\texttt{]} & \text{if } t = f(t_1, \ldots, t_n) \\ (\overline{t'}\ \texttt{in}\ \overline{R}) & \text{if } t = [t']_R. \end{cases} \tag{4}$$

Proposition 6. *Let $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i\in[1..p]}$ be a finite multiset of theories in $\mathcal{CR}$, with each $\Omega_i = (K, \Sigma_i, S_i)$. Then, for all theories $R_i \in \mathcal{R}$, terms $t \in (T^{\mathcal{R}}_{\Omega_i})_k$ and sorts s in $(S_i)_k$, $k \in K$,*

$$R_i \vdash^{\mathcal{R}} t : s \iff \texttt{MB-META}^{=} \vdash (\overline{t}\ \texttt{:}\ \overline{s}\ \texttt{in}\ \overline{R_i}) = \texttt{true}.$$

Similarly, for all terms $t, t' \in (T^{\mathcal{R}}_{\Omega_i})_k$, $k \in K$,

$$R_i \vdash^{\mathcal{R}} t = t' \iff \texttt{MB-META}^{=} \vdash (\overline{t}\ \texttt{=}\ \overline{t'}\ \texttt{in}\ \overline{R_i}) = \texttt{true}\,.$$

Proof. This proposition is a corollary of Props. 4 and 5. □

7 An Inductive Principle for Logically Proving Semantic Relations

We are now ready to prove in Prop. 7 below the main technical result in this paper, namely, that there is a class of metatheorems about membership equational logic theories which can be represented and logically proved as theorems about the initial model of the membership equational theory $\texttt{MB-META}^{=}$. As a corollary of this proposition we will obtain an inductive reasoning principle $(\overline{ind^{+}})$ for *logically* proving metatheorems about families of membership equational theories.

In order to simplify the presentation of the upcoming material, we introduce here some additional notation. Let $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i\in[1..p]}$ be a finite multiset of theories in $\mathcal{CR}$, with each $\Omega_i = (K, \Sigma_i, S_i)$. For all theories $R_i \in \mathcal{R}$ and terms $t \in T^{\mathcal{R}}_{\Omega_i}(X)$, we denote by $\overline{t}^{[X]}$ the reflective representation of t defined in (4), except that now variables $x \in X$ are replaced by variables $\overline{x}^{[X]} = x$ of the kind $\texttt{[Term]}$,[1] and we denote by $\overline{X}^{[X]}$ the set $\overline{X}^{[X]} \triangleq \{\overline{x}^{[X]} \mid x \in X\}$. In addition, for all theories $R_i \in \mathcal{R}$, and membership assertions $t\,\texttt{:}\,s$, with t in $T^{\mathcal{R}}_{\Omega_i}(X)$ and s in some $(S_i)_k$,

$$\overline{t\,\texttt{:}\,s}^{[R_i,X]} \triangleq (\overline{t}^{[X]}\ \texttt{:}\ \overline{s}\ \texttt{in}\ \overline{R_i}) = \texttt{true}\,,$$

and, similarly, for all equations $t = t'$, with t, t' in $T^{\mathcal{R}}_{\Omega_i}(X)$,

$$\overline{t = t'}^{[R_i,X]} \triangleq (\overline{t}^{[X]}\ \texttt{=}\ \overline{t'}^{[X]}\ \texttt{in}\ \overline{R_i}) = \texttt{true}\,.$$

[1] The key difference between $\overline{t}$ and $\overline{t}^{[X]}$ is that $\overline{t}$ is a *ground term* of sort $\texttt{Term}$, whereas $\overline{t}^{[X]}$ is a term of kind $\texttt{[Term]}$ with variables of the kind $\texttt{[Term]}$.

We can now define a representation function for metalogical statements, which satisfies the expected property, as shown in Prop. 7 below. Let $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i\in[1..p]}$ be a finite multiset of theories in $\mathcal{CR}$, with each $\Omega_i = (K, \Sigma_i, S_i)$. Let $\{k_1, \ldots, k_n\}$ be a finite multiset of kinds, with each k_i in K, let $\vec{x} = \{x_1, \ldots, x_n\}$ be a finite set of variables, with each x_i of kind k_i, and let τ be a metalogical statement of the form

$$\forall t_1 \in (T_{\Omega_1})_{k_1}. \ldots \forall t_n \in (T_{\Omega_n})_{k_n}. \, bexp(R_1 \vdash^{\mathcal{R}} \phi_1(\vec{t}), \ldots, R_p \vdash^{\mathcal{R}} \phi_p(\vec{t}))\,, \qquad (5)$$

where each $\phi_l(\vec{x})$ is an atomic $(\Omega_l, \mathcal{R})$-formula with free variables in $\vec{x}$. Then,

$$\overline{\tau} \triangleq \forall x_1. \ldots \forall x_n. (((x_1 \ \texttt{::}\ \overline{k_1} \ \texttt{in}\ \overline{R_1}) = \texttt{true} \wedge \cdots \wedge (x_n \ \texttt{::}\ \overline{k_n} \ \texttt{in}\ \overline{R_n}) = \texttt{true}) \Longrightarrow bexp(\overline{\phi_1(\vec{x})}^{[R_1,\vec{x}]}, \ldots, \overline{\phi_p(\vec{x})}^{[R_p,\vec{x}]}))\,,$$

where $\{x_1, \ldots, x_n\}$ are now variables of the kind `[Term]`.

Note that the class of metalogical statements of the form (5) includes, for example, all instances of the properties (1-a) in Def. 1, and (2-a) and (2-c) in Def. 2. In particular, the metalogical statement (1) is represented in $\texttt{MB-META}^{=}$ as the formula

$$\forall \texttt{N}.((\texttt{N} \ \texttt{::}\ \overline{\texttt{Num}} \ \texttt{in}\ \overline{\texttt{INT2}} = \texttt{true}) \Longrightarrow (\texttt{N} \ \texttt{:}\ \overline{\texttt{Int}} \ \texttt{in}\ \overline{\texttt{INT2}} = \texttt{true}) \Longrightarrow ((\texttt{N in}\ \overline{\texttt{INT2}}) \ \texttt{:}\ \overline{\texttt{Int}} \ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}))\,,$$

where `N` is a variable of the kind `[Term]`.

Proposition 7. *Let $\mathcal{R} = \{R_i\}_i = \{(\Omega_i, E_i)\}_{i\in[1..p]}$ be a finite multiset of theories in $\mathcal{CR}$, with each $\Omega_i = (K, \Sigma_i, S_i)$. For all metalogical statements τ of the form (5), τ holds iff* $\texttt{MB-META}^{=} \models\!\!\simeq \overline{\tau}$.

Proof. We first prove the $(\Rightarrow)$-direction of this proposition. Suppose that τ holds. Let $\sigma : \{x_1, \ldots, x_n\} \longrightarrow T_{\texttt{MB-META}^{=}}$ be a substitution such that, for $1 \leq i \leq n$,

$$\texttt{MB-META}^{=} \models\!\!\simeq (\sigma(x_i) \ \texttt{::}\ \overline{k_i} \ \texttt{in}\ \overline{R_i}) = \texttt{true}\,. \qquad (6)$$

We must prove that

$$\texttt{MB-META}^{=} \models\!\!\simeq \sigma\left(bexp(\overline{\phi_1(\vec{x})}^{[R_1,\vec{x}]}, \ldots, \overline{\phi_p(\vec{x})}^{[R_p,\vec{x}]})\right)\,.$$

Note that, since $(\sigma(x_i) \ \texttt{::}\ \overline{k_i} \ \texttt{in}\ \overline{R_i})$ is a ground term, (6) implies

$$\texttt{MB-META}^{=} \models (\sigma(x_i) \ \texttt{::}\ \overline{k_i} \ \texttt{in}\ \overline{R_i}) = \texttt{true}\,,$$

which, by completeness of membership equational logic, implies

$$\texttt{MB-META}^{=} \vdash (\sigma(x_i) \ \texttt{::}\ \overline{k_i} \ \texttt{in}\ \overline{R_i}) = \texttt{true}\,.$$

Thus, by Prop. 3, we know that, for $1 \leq i \leq n$, $\sigma(x_i) = \overline{w_i}$ for some $w_i \in (T_{\Omega_i})_{k_i}$. Note then that

$$\sigma\left(bexp(\overline{\phi_1(\vec{x})}^{[R_1,\vec{x}]}, \ldots, \overline{\phi_p(\vec{x})}^{[R_p,\vec{x}]})\right) = bexp(\overline{\phi_1(\vec{w})}^{[R_1,\emptyset]}, \ldots, \overline{\phi_p(\vec{w})}^{[R_p,\emptyset]}),$$

and that, by Prop. 6, for $1 \leq l \leq p$, $R_l \vdash^{\mathcal{R}} \phi_l(\vec{w})$ iff $\texttt{MB-META}^{=} \vdash \overline{\phi_l(\vec{w})}^{[R_l,\emptyset]}$. Since we are assuming that $bexp(R_1 \vdash^{\mathcal{R}} \phi_1(\vec{w}), \ldots, R_p \vdash^{\mathcal{R}} \phi_p(\vec{w}))$ holds, then

$$\texttt{MB-META}^{=} \vdash bexp(\overline{\phi_1(\vec{w})}^{[R_1,\emptyset]}, \ldots, \overline{\phi_p(\vec{w})}^{[R_p,\emptyset]}) \,,$$

and, by soundness of membership equational logic,

$$\texttt{MB-META}^{=} \models bexp(\overline{\phi_1(\vec{w})}^{[R_1,\emptyset]}, \ldots, \overline{\phi_p(\vec{w})}^{[R_p,\emptyset]}) \,,$$

as required.

The proof of the ($\Leftarrow$)-direction is similar. In particular, consider for any terms $\{w_1, \ldots, w_n\}$ the substitution $\sigma : \{x_1, \ldots, x_n\} \longrightarrow T_{\texttt{MB-META}^{=}}$ given by $\sigma(x_i) = \overline{w_i}$, for $1 \leq i \leq n$. □

As corollaries of Prop. 7 we can prove the reflective versions of Rem. 1 and Prop. 1, which we will denote, respectively, as Rem. $\overline{1}$, and Prop. $\overline{1}$. Both are obtained by replacing each metalogical statement ϕ in Rem. 1 and Prop. 1 by its logical representation $\overline{\phi}$ in $\texttt{MB-META}^{=}$. Of course, this is key for our purposes, since it automatically gives us an inductive reasoning principle ($\overline{ind^{+}}$), and a case analysis reasoning principle ($\overline{case^{+}}$), for proving metalogical statements about membership equational theories represented as logical statements in $\texttt{MB-META}^{=}$. Moreover, since Rem. $\overline{1}$ and Prop. $\overline{1}$ mirror their metalogical counterparts, the metalogical proofs based on the latter will also be mirrored by the logical proofs based on the former. As an example of this, we *logically* prove in the appendix, using the induction principle ($\overline{ind^{+}}$), that INT_2 satisfies property (2-c) with respect to INT_1.

8 Conclusion

The work presented is based on the ideas proposed in [1] for formal metareasoning using reflection. Here we extend the metareasoning principles introduced in [1], increasing their applicability as we show in a case study. The reader can find in [1] a detailed discussion on tradeoffs and limitations of reflective metalogical frameworks, and a survey of related work.

One of the advantages of formal metareasoning based on reflection is that it can be carried out using already existing logical reasoning tools. Our experience shows also that the logical proofs of metatheorems using reflection mirror their standard metalogical proofs. In this regard, we plan to use our results to extend the ITP tool [3, 4], which is an interactive inductive theorem prover for membership equational theories, with metareasoning capabilities, so that it can be used, for example, as a methodological tool for software development.

Acknowledgments

We thank David Basin and José Meseguer for many discussions on using reflection for formal metareasoning. We also thank two anonymous referees for their helpful comments on ways of improving the presentation of our results.

References

1. D. Basin, M. Clavel, and J. Meseguer. Reflective metalogical frameworks. *ACM Transactions on Computational Logic*, 2004. To appear. `http://www.acm.org/pubs/tocl/accepted.html`.
2. A. Bouhoula, J.-P. Jouannaud, and J. Meseguer. Specification and proof in membership equational logic. *Theoretical Computer Science*, 236:35–132, 2000.
3. M. Clavel. *Reflection in Rewriting Logic: Metalogical Foundations and Metaprogramming Applications*. CSLI Publications, 2000.
4. M. Clavel. The ITP tool's home page. `http://geminis.sip.ucm.es/~clavel/itp`, 2004.
5. M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, and J. F. Quesada. Maude: Specification and programming in rewriting logic. *Theoretical Computer Science*, 285:187–243, 2002.
6. M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, and C. Talcott. Maude Manual (Version 2.1). Manual distributed as documentation of the Maude system. `http://maude.cs.uiuc.edu`, 2004.
7. M. Clavel, N. Martí-Oliet, and M. Palomino. Formalizing and proving semantic relations between specifications by reflection (extended version). `http://geminis.sip.ucm.es/~clavel/pubs/pubs.html`, 2004.
8. M. Clavel and J. Meseguer. Axiomatizing reflective logics and languages. In G. Kiczales, editor, *Proc. Reflection'96*, pages 263–288. Xerox PARC, 1996.
9. M. Clavel, J. Meseguer, and M. Palomino. Reflection in membership equational logic, many-sorted equational logic, Horn logic with equality, and rewriting logic. In F. Gadducci and U. Montanari, editors, *Proc. Fourth International Workshop on Rewriting Logic and its Applications*, volume 71 of *Electronic Notes in Theoretical Computer Science*, pages 63–78. Elsevier, 2002. `http://geminis.sip.ucm.es/~clavel/pubs/pubs.html`.
10. H. Ehrig and B. Mahr. *Fundamentals of Algebraic Specification 1*, volume 6 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, 1985.
11. J. Loeckx, H.-D. Ehrich, and M. Wolf. *Specification of Abstract Data Types*. J. Wiley & Sons and B.G. Teubner, 1996.
12. J. Meseguer. Membership algebra as a logical framework for equational specification. In F. Parisi-Presicce, editor, *Proc. WADT'97*, volume 1376 of *LNCS*, pages 18–61. Springer-Verlag, 1998.

Appendix

We show how Fact 1 below, that is, the representation of the metalogical statement (1) as a logical statement about the initial model of $\texttt{MB-META}^{=}$, can be logically proved using the inductive principle ($\overline{ind^{+}}$), along with the reflective properties of membership equational logic. Our proof mirrors at the logical level the metalogical proof of (1), that we omit here for the sake of space limitations; this proof can be found in [7].

Fact 1.

$$\texttt{MB-META}^{=} \models\!\!\sim \forall \texttt{N}.(\texttt{N} :: \overline{\texttt{Num}}\ \texttt{in}\ \overline{\texttt{INT2}} = \texttt{true} \implies (\texttt{N} : \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT2}} = \texttt{true}) \implies ((\texttt{N}\ \texttt{in}\ \overline{\texttt{INT2}}) : \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}))\,,$$

where `N` is a variable of the kind `[Term]`.

Proof. By $(\overline{ind^+})$, we can prove the theorem by showing:

$$\begin{aligned}
&\texttt{MB-META}^{=} \models\!\simeq ((\overline{\texttt{0}}\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}) && (7)\\
&\qquad \wedge\ \forall \texttt{N}.(\texttt{N}\ ::\ \overline{\texttt{Num}}\ \texttt{in}\ \overline{\texttt{INT2}} = \texttt{true}\\
&\qquad\quad \Longrightarrow ((\texttt{N}\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}) && (8)\\
&\qquad\quad \Longrightarrow ((\overline{\texttt{s}}[\texttt{N}]\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}))\\
&\qquad \wedge\ \forall \texttt{N}.(\texttt{N}\ ::\ \overline{\texttt{Num}}\ \texttt{in}\ \overline{\texttt{INT2}} = \texttt{true}\\
&\qquad\quad \Longrightarrow ((\texttt{N}\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}) && (9)\\
&\qquad\quad \Longrightarrow ((\overline{\texttt{p}}[\texttt{N}]\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}))\,,
\end{aligned}$$

where N is a variable of the kind [Term]. Note that (7) holds by Prop. 6 (using soundness of membership equational logic). Regarding (8) and (9), their proofs are similar; we show here only the proof of (8). It is a fact[2] that, (8) holds if

$$\begin{aligned}
&\texttt{MB-META}^{=} \models\!\simeq \forall \texttt{N}.(\texttt{N}\ ::\ \overline{\texttt{Num}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true} \Longrightarrow (\texttt{N}\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}) && (10)\\
&\qquad\qquad \Longrightarrow ((\overline{\texttt{s}}[\texttt{N}]\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}))\,,
\end{aligned}$$

which, by Rem. $\overline{1}$, is equivalent to

$$\begin{aligned}
&\texttt{MB-META}^{=} \models\!\simeq \forall \texttt{N}.(\texttt{N}\ ::\ \overline{\texttt{Num}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true} \Longrightarrow (\texttt{N}\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}) && (11)\\
&\qquad\qquad \Longrightarrow ((\overline{\texttt{s}}[\texttt{N}\ \texttt{in}\ \overline{\texttt{INT1}}]\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}))\,.
\end{aligned}$$

To prove (11) we can use again $(\overline{ind^+})$, and reduce its proof to showing:

$$\begin{aligned}
&\texttt{MB-META}^{=} \models\!\simeq \forall \texttt{N}.(\texttt{N}\ ::\ \overline{\texttt{Num}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true} \Longrightarrow (\texttt{N}\ :\ \overline{\texttt{Nat}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}) && (12)\\
&\qquad\qquad \Longrightarrow ((\overline{\texttt{s}}[\texttt{N}\ \texttt{in}\ \overline{\texttt{INT1}}]\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}))\\
&\qquad\qquad \wedge\ \forall \texttt{N}.(\texttt{N}\ ::\ \overline{\texttt{Num}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true} \Longrightarrow (\texttt{N}\ :\ \overline{\texttt{Neg}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}) && (13)\\
&\qquad\qquad \Longrightarrow ((\overline{\texttt{s}}[\texttt{N}\ \texttt{in}\ \overline{\texttt{INT1}}]\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}))
\end{aligned}$$

The proofs of (12) and (13) are similar; we show here only the proof of (13). By $(\overline{case^+})$ and Rem. $\overline{1}$, we can reduce proving (13) to showing:

$$\begin{aligned}
&\texttt{MB-META}^{=} \models\!\simeq (\overline{\texttt{s}}[\overline{\texttt{0}}]\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true} && (14)\\
&\qquad \wedge\ \forall \texttt{N}.(\texttt{N}\ ::\ \overline{\texttt{Num}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true} \Longrightarrow (\texttt{N}\ :\ \overline{\texttt{Neg}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}) && (15)\\
&\qquad\quad \Longrightarrow ((\overline{\texttt{s}}[\overline{\texttt{p}}[\texttt{N}]]\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true}))
\end{aligned}$$

Note that (14) holds by Prop. 6 (using soundness of membership equational logic). Regarding (15), let $\sigma : \{\texttt{N}\} \longrightarrow T_{\texttt{MB-META}^{=}}$ be a substitution such that $(\sigma(\texttt{N})\ ::\ \overline{\texttt{Num}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true})$ and $(\sigma(\texttt{N})\ :\ \overline{\texttt{Neg}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true})$ hold in the initial model of $\texttt{MB-META}^{=}$. Thus, by Prop. 3, $\sigma(\texttt{N}) = \overline{N}$ for some term N of kind Num, and, by Prop. 4, $INT_1 \vdash N : Neg$. Finally, note that, since $INT_2 \vdash s(p(N)) = N$, then, by Prop. 6 (using again soundness of membership equational logic),

$$\texttt{MB-META}^{=} \models\!\simeq (\overline{\texttt{s}}[\overline{\texttt{p}}[\overline{N}]]\ \texttt{in}\ \overline{\texttt{INT2}})\ :\ \overline{\texttt{Int}}\ \texttt{in}\ \overline{\texttt{INT1}} = \texttt{true})\,.$$

□

[2] This fact is an instance of the reflective counterpart of a general metareasoning principle for reducing metalogical statements to a form such that (ind^+) can be applied to them. For the sake of space limitations, we omit here the proposition that states this principle, and its proof, that can be found in [7].