



**HAL**  
open science

## Some techniques for reasoning automatically on co-inductive data structures

Nicolas Peltier

► **To cite this version:**

Nicolas Peltier. Some techniques for reasoning automatically on co-inductive data structures. Journal of Logic and Computation, 2024, 34 (3), pp.429-464. 10.1093/LOGCOM/EXAD028 . hal-04618309

**HAL Id: hal-04618309**

**<https://hal.science/hal-04618309>**

Submitted on 20 Jun 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Some Techniques for Reasoning Automatically on Co-Inductive Data Structures

Nicolas Peltier

Univ. Grenoble Alpes, CNRS, LIG, F-38000 Grenoble France

## Abstract

Some techniques are proposed for reasoning on co-inductive structures. First, we devise a sound axiomatization of (conservative extensions) of such structures, thus reducing the problem of checking whether a formula admits a co-inductive model to a first-order satisfiability test. We devise a class of structures, called regularly co-inductive, for which the axiomatization is complete (for other co-inductive structures, the proposed axiomatization is sound, but not complete). Then, we propose proof calculi for reasoning on such structures. We first show that some of the axioms mentioned above can be omitted if the inference rules are able to handle rational terms. Furthermore, under some conditions, some other axioms may be replaced by an additional inference rule that computes the solutions of fixpoint equations. Finally, we show that a stronger completeness result can be established under some additional conditions on the signature.

## 1 Introduction

In automated reasoning, a lot of attention has been given to the handling of *inductive data structures*, i.e., of structures defined as the least fixpoint of some monotonic operator. Standard approaches use rewriting techniques [7, 8, 10, 16] and more recent works combine inductive reasoning with efficient proof procedures such as the superposition calculus [13, 14, 17] or SMT-solving [15, 24]. Cyclic proof systems are also used [9]. Comparatively, the problem of reasoning automatically on *co-inductive structures* did not receive as much attention. Co-induction (see, e.g., [25]) is dual to induction and allows one to reason on structures defined as the greatest fixpoint of an operator, such as streams or infinite trees. Co-inductive structures are usually defined by considering a specific set of function symbols called *constructors* and allowing for infinite terms built on such constructors. Such structures are ubiquitous in mathematics and computer science. We briefly mention some existing approaches (with no pretension to exhaustivity). Co-inductive datatypes have been integrated in proof assistants such as Isabelle/HOL (see for instance [5]). The theorem prover CVC4 [4] and the program verification tool Dafny [19] both offer some support for reasoning on co-inductive datatypes. Co-induction can be integrated in logical calculi by using suitable explicit co-induction schemes [23] and/or cyclic proof systems [12]. Cyclic co-inductive proof systems have also been considered in rewrite logic [21]. Co-induction is also useful in logic programming: in [26],

logic programs combining induction and co-induction are considered, and in [1] a language for programming with infinite structures defined by observations is proposed and its operational semantics is defined.

While most existing approaches to automatize co-inductive reasoning devise specific inference rules and proof procedures, the approach we investigate in the present paper is different: it consists in reducing co-inductive reasoning to first-order reasoning. The goal is to allow for the combination of co-induction with standard logical reasoning and to enable the use of the most efficient systems developed for first-order theorem proving. The approach is related to that of [22], in which a complete first-order axiomatization of infinite trees is introduced, but our framework is more general, as it allows for defined functions and predicates. We emphasize that we do not aim at capturing co-inductive reasoning in its full generality: our aim is only to make theorem provers able to handle infinite data structures, where the equality predicate is defined co-inductively.

Our approach is similar to that of [6], in which axioms and superposition-related inference rules are proposed to reason on co-inductive data structures. However, the axioms and rules in [6] only capture some specific properties of co-inductive data structures (listed in Section 3.5), in particular the fact that every fixpoint equation (defined on constructors) admits a unique solution. The proof procedure in [6] is complete only w.r.t. these properties. It is not always able, for instance, to prove that two bisimilar terms (i.e., two terms that agree on all positions) are equal. For example, if  $c$  denotes a constructor, then the procedure is able to derive the equality  $a \approx b$  from the axioms  $\{a \approx c(a, a), b \approx c(b, b)\}$ , by detecting that  $a$  and  $b$  are both solutions of the same fixpoint equation  $x \approx c(x, x)$ , which entails that these two terms must be equal, but it is not able to derive the same equality from the set of axioms  $\{a \approx c(a, b), b \approx c(b, a)\}$ , although it is clear that the axioms entail that  $a$  and  $b$  are bisimilar terms, hence they should be equal by the co-induction principle. Such an equality can only be established by mutual co-induction.

In this paper, we devise new techniques for reasoning on co-inductive structures that capture additional properties of these structures (compared with [6]) and in particular that are able to infer that bisimilar terms are equals. We focus on finitely branching trees, and we design a finite axiomatization of conservative extensions of co-inductive structures, and we prove that it is sound and complete w.r.t. a class of structures that we call *regularly co-inductive*. This result allows one to reduce the problem of checking that a formula admits a regularly co-inductive interpretation to a first-order satisfiability check, which can be performed by any first-order theorem prover. The proposed axiomatization can also be used to reason on co-inductive structures that are not regularly co-inductive. In this case, it is sound, but not complete (no complete first-order axiomatization exists for co-inductive structures, see Proposition 46). We prove that the obtained proof procedure is strictly more general than that of [6], in the sense that there exist formulas that cannot be proven using the axioms and inference rules in [6], but that can be established using the axioms proposed in the present work. Conversely, the structures we consider fulfill all the axioms in [6] (with the exception of the axiom stating that the domain is infinite, which may be falsified in some trivial cases).

Building on these results, we then define resolution-based proof calculi for co-inductive reasoning. The idea is to replace some of the previously defined axioms by suitable inference rules. First, we prove that, if the unification algorithm is

able to cope with rational terms, then some of the axioms may be omitted – namely those asserting the existence of an interpretation for each rational term. Second, if every constructor admits at most one argument of some co-inductive sort (which entails that all infinite terms admit at most one infinite branch) then the axioms asserting the unicity of the interpretation of a rational term can also be omitted and replaced by a new inference rule that computes the solution of fixpoint equations. Finally, we identify a class of formulas for which satisfiability for co-inductive and regularly co-inductive structures coincides, which increases the applicability of the proposed approach.

## 2 Formulas with Infinite Terms

In the present section, we define the syntax and semantics of infinite terms and formulas built on them. We also devise conditions on interpretations ensuring that such terms can be associated with a unique value.

### 2.1 Syntax

We recall some necessary definitions about infinite terms<sup>1</sup>. Let  $\mathcal{S}$  be a finite set of *sort symbols*, partitioned into two sets:  $\mathcal{S} = \mathcal{S}_{\text{ci}} \cup \mathcal{S}_{\text{st}}$ , with  $\mathcal{S}_{\text{ci}} \cap \mathcal{S}_{\text{st}} = \emptyset$ . The symbols in  $\mathcal{S}_{\text{ci}}$  and  $\mathcal{S}_{\text{st}}$  are the *co-inductive sorts* and the *standard sorts*, respectively. Let  $\Sigma$  be a finite set of *function symbols* (signature). Each symbol in  $\Sigma$  is associated with a unique *profile* in  $\mathcal{S}^+$ . We write  $f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$  (with  $\mathbf{s}_1, \dots, \mathbf{s}_n, \mathbf{s} \in \mathcal{S}$ ) to state that the profile of  $f$  is  $(\mathbf{s}_1, \dots, \mathbf{s}_n, \mathbf{s})$ . The natural number  $n$  is the *arity* of  $f$  and is denoted by  $\#(f)$ , and  $\mathbf{s}$  is its *co-domain*. A function of arity 0 is called a *constant symbol*. Let  $\mathcal{C}$  be a set of *constructors*, such that  $\mathcal{C} \subseteq \Sigma$  and the co-domain of each symbol  $c \in \mathcal{C}$  is in  $\mathcal{S}_{\text{ci}}$ . Without loss of generality, we assume (by reordering arguments if needed) that the profile of every constructor  $c$  is of the form  $\mathbf{s}_1, \dots, \mathbf{s}_n, \mathbf{s}'_1, \dots, \mathbf{s}'_m \rightarrow \mathbf{s}$ , with  $n \geq 0, m \geq 0, \{\mathbf{s}_1, \dots, \mathbf{s}_n\} \subseteq \mathcal{S}_{\text{ci}}$  and  $\{\mathbf{s}'_1, \dots, \mathbf{s}'_m\} \subseteq \mathcal{S}_{\text{st}}$ . The number  $n$  is denoted by  $\#_{\text{ci}}(c)$  (note that  $\#_{\text{ci}}(c) \leq \#(c) = n + m$ ). We assume that there exists at least one sort  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$  with two distinct constructors of co-domain  $\mathbf{s}$  (this assumption is for technical convenience only and simplifies the proof of Theorem 26 as explained in footnote 4; it can be enforced if needed by adding a fresh sort symbol  $\mathbf{s}$  and two distinct constructors  $c : \rightarrow \mathbf{s}$  and  $d : \rightarrow \mathbf{s}$ ). Let  $\mathcal{V}$  be a set of *variables*. Each variable is associated with a unique sort symbol  $\mathbf{s}$  and we denote by  $\mathcal{V}_{\mathbf{s}}$  the set of variables of sort  $\mathbf{s}$ .

A *position* is an element of  $\mathbb{N}^*$ . We denote by  $|p|$  the length of the position  $p$ , by  $\varepsilon$  the empty position and by  $p.q$  the concatenation of the positions  $p$  and  $q$ . For any  $i, j \in \mathbb{N}$   $i^j$  denotes the position  $i \dots i$  ( $j$  times). If  $p$  and  $q$  are (possibly infinite) sequences, we write  $p \preceq q$  (resp.  $p \prec q$ ) to state that  $p$  is a prefix (resp. a strict prefix) of  $q$ .

Terms are (possibly infinite) trees labeled by function symbols or variables, and satisfying some syntactic conditions. Formally, they can be viewed as functions mapping positions to symbols (this approach is standard, see for instance [11]):

<sup>1</sup>Some more abstract formulations are possible, however, they do not suit our purposes, since our goal is to eventually define rules operating on concrete terms.

**Definition 1 (Term).** A term  $t$  is a partial function from  $\mathbb{N}^*$  to  $\Sigma \cup \mathcal{V}$  satisfying the following conditions:

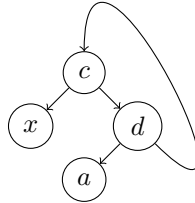
- The domain of  $t$  is closed under prefixes, i.e., if  $p \in \text{dom}(t)$  and  $q \preceq p$  then  $q \in \text{dom}(t)$ .
- If  $t(p) = f \in \Sigma$  then:  $p.i \in \text{dom}(t) \iff i \in \{1, \dots, \#(f)\}$ .

Let  $\text{sort}_t$  be the total function of domain  $\text{dom}(t)$  defined as follows:  $\text{sort}_t(p) \stackrel{\text{def}}{=} \mathbf{s}$  if  $t(p) \in \mathcal{V}_{\mathbf{s}}$  or if  $t(p)$  is a function of co-domain  $\mathbf{s}$ . The term  $t$  is well-typed if, for every position  $p$  such that  $t(p) = f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$  and for every  $i \in \{1, \dots, \#(f)\}$ , we have  $\text{sort}_t(p.i) = \mathbf{s}_i$ . If  $t$  is well-typed then  $\text{sort}_t(\varepsilon)$  is called the sort of  $t$ .

A branch in  $t$  is a (possibly infinite) sequence of natural numbers  $\pi$  such that, for every position  $p$ :  $p \preceq \pi \implies p \in \text{dom}(t)$ , and  $\pi \prec p \implies p \notin \text{dom}(t)$ .

A term  $t$  is ground if  $t(p) \notin \mathcal{V}$  holds for all  $p \in \text{dom}(t)$ , finite iff  $\text{dom}(t)$  is finite, and admissible if non-constructor functions occur only finitely often along all branches in the term, i.e., for every infinite branch  $\pi$  in  $t$ , there exists a position  $p \prec \pi$  such that, for every position  $q$ :  $p \preceq q \prec \pi \implies t(q) \in \mathcal{C}$ . Note that every finite term is admissible. A term  $t$  is called a constructor term if for all  $p \in \text{dom}(t)$ :  $t(p) \in \mathcal{C} \cup \mathcal{V}$ . A position  $p$  is a constructor position in  $t$  if  $t(q) \in \mathcal{C}$  for all  $q \prec p$ .

**Example 2.** Let  $t$  be the term such that  $\text{dom}(t) = \{2^i, 2^i.1 \mid i \in \mathbb{N}\}$ ,  $t(2^{2^i}) = c$ ,  $t(2^{2^i+1}) = d$ ,  $t(2^{2^i}.1) = x$ , and  $t(2^{2^i+1}.1) = a$  (with  $c, d \in \mathcal{C}$ ). We have  $t = c(x, d(a, t))$ , and this term may be depicted graphically as follows:



If  $a \notin \mathcal{C}$ , then  $\varepsilon, 2, 2.2, \dots$  are constructor positions in  $t$  (but not 1 or 2.1).

The following definition is useful to define the notion of a subterm:

**Definition 3.** For every function  $f$  mapping positions to some codomain and for every position  $p \in \text{dom}(f)$ , we denote by  $f|_p$  the function defined as follows:  $\text{dom}(f|_p) \stackrel{\text{def}}{=} \{q \mid p.q \in \text{dom}(f)\}$  and for every  $q \in \text{dom}(f|_p)$ :  $f|_p(q) \stackrel{\text{def}}{=} f(p.q)$ .

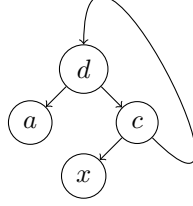
**Proposition 4.** If  $t$  is a well-typed term and  $p \in \text{dom}(t)$ , then  $t|_p$  is a well-typed term, and  $\text{sort}_{t|_p} = \text{sort}_t|_p$ . In particular,  $t|_p$  is of sort  $\text{sort}_t(p)$ .

*Proof.* Immediate. □

We shall silently assume, in the remainder of the paper, that all the considered terms are admissible and well-typed.

**Definition 5.** A term  $t$  is a subterm of a term  $s$  if  $t = s|_p$ , for some position  $p \in \text{dom}(s)$ . It is proper if  $p \neq \varepsilon$ . The term  $s$  is rational if it admits finitely many pairwise distinct subterms, in which case we denote by  $\text{size}(s)$  the number of pairwise distinct subterms in  $s$ .

**Example 6.** The term  $t$  of Example 2 has 4 subterms:  $t$ ,  $x$ ,  $a$  and the term  $s = t|_2 = d(a, c(x, s))$  that can be depicted as follows:



We have  $\text{size}(t) = \text{size}(s) = 4$  and  $\text{size}(x) = \text{size}(a) = 1$ .

A term may be a proper subterm of itself, in which case it is necessarily infinite. The set of ground rational admissible terms of sort  $\mathbf{s}$  is denoted by  $\mathcal{T}_{\mathbf{s}}^g$ . Let  $\mathcal{T}^g \stackrel{\text{def}}{=} \bigcup_{\mathbf{s} \in \mathcal{S}} \mathcal{T}_{\mathbf{s}}^g$ . As usual, we denote by  $t[s]_p$  the term obtained from  $t$  by replacing the subterm at position  $p$  by  $s$ , formally defined as follows.

**Definition 7.** For all functions  $t, s$  mapping positions to symbols and for every position  $p \in \text{dom}(t)$ , we denote by  $t[s]_p$  the function defined as follows:  $\text{dom}(t[s]_p) = \{q \in \text{dom}(t) \mid p \not\leq q\} \cup \{p.q \mid q \in \text{dom}(s)\}$ ;  $t[s]_p(q) = t(q)$  if  $q \in \text{dom}(t)$  and  $p \not\leq q$ ; and  $t[s]_p(p.q) = s(q)$  if  $q \in \text{dom}(s)$ .

**Proposition 8.** If  $t, s$  are well-typed terms,  $p \in \text{dom}(t)$  and  $\text{sort}_{\mathbf{s}}(\varepsilon) = \text{sort}_t(p)$  then  $t[s]_p$  is a well-typed term, and  $\text{sort}_{t[s]_p} = \text{sort}_t[\text{sort}_s]_p$ .

*Proof.* Immediate. □

As usual, if  $t_i$  is a term of sort  $\mathbf{s}_i$  (for  $i = 1, \dots, n$ ) and  $f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$ , then  $f(t_1, \dots, t_n)$  denotes the term  $t$  such that  $\text{dom}(t) \stackrel{\text{def}}{=} \{\varepsilon, i.p \mid i \in \{1, \dots, n\}, p \in \text{dom}(t_i)\}$ ,  $t(\varepsilon) \stackrel{\text{def}}{=} f$ , and for all  $i = 1, \dots, n$  and  $p \in \text{dom}(t_i)$ :  $t(i.p) \stackrel{\text{def}}{=} t_i(p)$ . It is clear that  $t|_i = t_i$ .

We assume that  $\mathcal{S}_{\text{st}}$  contains a special sort  $\text{bool}$  such that there is no function  $f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$  with  $\mathbf{s}_i = \text{bool}$  for some  $i = 1, \dots, n$ . If  $f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \text{bool}$  then  $f$  is called a *predicate symbol*. We assume that the signature contains one symbol  $\approx_{\mathbf{s}} : \mathbf{s}, \mathbf{s} \rightarrow \text{bool}$  for each  $\mathbf{s} \in \mathcal{S} \setminus \{\text{bool}\}$ , used in infix notation. The index is often omitted, i.e., if  $t$  and  $s$  are two terms of sort  $\mathbf{s}$ , then we write  $t \approx s$  instead of  $t \approx_{\mathbf{s}} s$ .

**Definition 9 (Formulas).** The set of formulas is inductively defined as follows: a formula is either a term of sort  $\text{bool}$  (called an atom), or an expression of the form  $(\phi_1 \vee \phi_2)$ ,  $\neg\phi$  or  $\exists x.\phi$ , where  $\phi_1, \phi_2, \phi$  are formulas, and  $x$  is a variable. As usual  $\forall x.\phi$ ,  $\phi_1 \wedge \phi_2$ ,  $\phi_1 \Rightarrow \phi_2$ , and  $\phi_1 \Leftrightarrow \phi_2$  are shorthands for  $\neg\exists x.\neg\phi$ ,  $\neg(\neg\phi_1 \vee \neg\phi_2)$ ,  $\neg\phi_1 \vee \phi_2$ , and  $(\phi_1 \Rightarrow \phi_2) \wedge (\phi_2 \Rightarrow \phi_1)$ , respectively. A formula is finite (resp. rational) if it contains no infinite (resp. irrational) term.

In practice input formulas will usually be finite. Infinite rational formulas will be produced from finite ones by the inference rules in Section 4.

## 2.2 Semantics

We define the semantics of the language and we introduce restricted classes of interpretations, called (*regularly*) *co-inductive*. Informally, a (regularly) co-inductive structure interprets constructors as injective functions with disjoint ranges, and fulfills additional conditions ensuring that every (rational) term can be associated with a unique value.

**Definition 10.** An interpretation  $\mathcal{I}$  is a function mapping every sort symbol  $\mathbf{s}$  to a non empty set  $\mathbf{s}^{\mathcal{I}}$  (with  $\text{bool}^{\mathcal{I}} = \{\top, \perp\}$ ), every variable  $x \in \mathcal{V}_{\mathbf{s}}$  to an element  $x^{\mathcal{I}}$  of  $\mathbf{s}^{\mathcal{I}}$  and every function symbol  $f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$  to a total function  $f^{\mathcal{I}}$  from  $\mathbf{s}_1^{\mathcal{I}}, \dots, \mathbf{s}_n^{\mathcal{I}}$  to  $\mathbf{s}^{\mathcal{I}}$ , where  $\approx_{\mathbf{s}}^{\mathcal{I}}$  is the equality on  $\mathbf{s}$ , i.e.,  $\approx_{\mathbf{s}}^{\mathcal{I}} = \{(\zeta, \zeta) \mid \zeta \in \mathbf{s}^{\mathcal{I}}\}$ . If  $t$  is finite, then we denote by  $[t]^{\mathcal{I}}$  the value of the term  $t$  in  $\mathcal{I}$ , defined inductively on  $t$ , as usual. An interpretation  $\mathcal{I}'$  is an associate of  $\mathcal{I}$  if  $\mathcal{I}$  and  $\mathcal{I}'$  coincide on all symbols except (possibly) on variables.

Infinite terms will be interpreted as the solutions of (mutual) fixpoint equations, for instance the interpretation of the infinite term  $t$  such that  $t = c(t)$  is the fixpoint of the function  $c^{\mathcal{I}}$ . To ensure that the interpretation is well-defined, we need to ensure that all such equations admit a unique solution. This motivates the following definition.

**Definition 11.** Let  $\mathcal{I}$  be an interpretation and let  $t$  be a term. A labeling function for  $t$  w.r.t.  $\mathcal{I}$  is a function  $\mu$  mapping every position  $p \in \text{dom}(t)$  to an element of  $\text{sort}_t(p)^{\mathcal{I}}$  satisfying the following conditions, for every  $p \in \text{dom}(t)$ :

1.  $t(p) \in \mathcal{V} \implies \mu(p) = t(p)^{\mathcal{I}}$  (note that  $t(p)^{\mathcal{I}}$  is defined since  $t(p)$  is a variable);
2.  $t(p) = f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s} \implies \mu(p) = f^{\mathcal{I}}(\mu(p.1), \dots, \mu(p.n))$  (by Definition 1,  $p.i \in \text{dom}(t)$ , for all  $i = 1, \dots, n$ ).

It is regular if it satisfies, moreover, the following property:

3. For every subterm  $s$  of  $t$ , the set  $\{\mu(p) \mid t|_p = s\}$  is finite.

It is easy to check that every finite term admits exactly one labeling function (w.r.t. every interpretation), which may be defined by induction on the position, using Conditions 1 and 2 in Definition 11, and that this function is trivially regular. The rôle and the importance of Condition 3 will be discussed in Section 5. We will show that completeness cannot be obtained if this condition is removed, except if the signature satisfies some additional conditions.

**Example 12.** Let  $t = c(x, t)$  be an infinite term with  $c : \mathbf{s}, \mathbf{s} \rightarrow \mathbf{s} \in \mathcal{C}$ . Let  $\mathcal{I}$  be the interpretation with  $\mathbf{s}^{\mathcal{I}} = \mathbb{Z}$ ,  $c^{\mathcal{I}}(x, y) = x + y$  and  $x^{\mathcal{I}} = 0$ . Then  $\text{dom}(t) = \{2^i.1, 2^i \mid i \geq 0\}$  with  $t|_{2^i} = t$  and  $t|_{2^i.1} = x$ , and the function  $\mu$  such that  $\mu(2^i.1) = 0$  and  $\mu(2^i) = 1$  is a labeling function (since  $\mu(2^i.1) = x^{\mathcal{I}}$  and  $\mu(2^i.1) + \mu(2^i.2) = 0 + 1 = \mu(2^i)$ ). It is regular, as its range is finite. If  $\mathcal{J}$  is an associate of  $\mathcal{I}$  such that  $x^{\mathcal{J}} = 1$ , then  $t$  admits no regular labeling function. Indeed, assume that such a function  $\nu$  exists. We have  $\nu(2^i) = c^{\mathcal{I}}(\nu(2^i.1), \nu(2^i.2)) = 1 + \nu(2^i.2) > \nu(2^{i+1})$ , hence the set  $\{\nu(2^i) \mid i \geq 0\} = \{\nu(\varepsilon) - i \mid i \geq 0\}$  is infinite.

A labeling function for a term  $t$  defines a labeling function for every subterm of  $t$ :

**Proposition 13.** *Let  $t$  be a term and let  $\mu$  be a (regular) labeling function for  $t$  w.r.t. an interpretation  $\mathcal{I}$ . For every  $p \in \text{dom}(t)$ , the function  $\mu|_p$  (as defined in Definition 3) is a (regular) labeling function for  $t|_p$ .*

*Proof.* Immediate. □

**Definition 14.** *An interpretation is  $\mathcal{C}$ -normal if it satisfies the following conditions:*

1. *For all constructors  $c$ ,  $c^{\mathcal{I}}$  is injective.*
2. *The ranges of distinct constructors are disjoint: if  $c : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$  and  $d : \mathbf{t}_1, \dots, \mathbf{t}_m \rightarrow \mathbf{t}$  are distinct constructors, then for all  $\zeta_i \in \mathbf{s}_i^{\mathcal{I}}$  (for  $i = 1, \dots, n$ ) and  $\xi_j \in \mathbf{t}_j^{\mathcal{I}}$  (for  $j = 1, \dots, m$ ),  $c^{\mathcal{I}}(\zeta_1, \dots, \zeta_n) \neq d^{\mathcal{I}}(\xi_1, \dots, \xi_m)$ .*
3. *All elements of co-inductive sorts must lie in the range of some constructor, i.e., for all  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ , and for all  $\zeta \in \mathbf{s}^{\mathcal{I}}$ , there exist  $c : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s} \in \mathcal{C}$  and  $\zeta_i \in \mathbf{s}_i^{\mathcal{I}}$  (for  $i = 1, \dots, n$ ) such that  $\zeta = c^{\mathcal{I}}(\zeta_1, \dots, \zeta_n)$ .*

**Definition 15.** *An interpretation  $\mathcal{I}$  is co-inductive if it is  $\mathcal{C}$ -normal and if, for every (admissible, possibly non rational) term  $t$  and for every associate  $\mathcal{J}$  of  $\mathcal{I}$ , there exists exactly one labeling function  $t^{\mathcal{J}}$  for  $t$  w.r.t.  $\mathcal{J}$ .*

*An interpretation  $\mathcal{I}$  is regularly co-inductive if it is  $\mathcal{C}$ -normal and if, for every (admissible) rational term  $t$  and for every associate  $\mathcal{J}$  of  $\mathcal{I}$ , there exists exactly one regular labeling function  $t^{\mathcal{J}}$  for  $t$  w.r.t.  $\mathcal{J}$ .*

*In both cases, the interpretation of the term  $t$  in  $\mathcal{I}$  is then defined as follows:  $[t]^{\mathcal{I}} \stackrel{\text{def}}{=} t^{\mathcal{I}}(\varepsilon)$ .*

**Proposition 16.** *All co-inductive interpretations are regularly co-inductive.*

*Proof.* Let  $\mathcal{I}$  be a co-inductive interpretation. Let  $t$  be an admissible regular term and let  $\mathcal{J}$  be an associate of  $\mathcal{I}$ . By definition, there exists a unique labeling function  $t^{\mathcal{J}}$  for  $t$  w.r.t.  $\mathcal{J}$ . Moreover,  $t^{\mathcal{J}}$  is regular: indeed, for all subterms  $s$  of  $t$  and for all positions  $p, q$  in  $t$  with  $t|_p = t|_q = s$ , by Proposition 13,  $t^{\mathcal{J}}|_p$  and  $t^{\mathcal{J}}|_q$  are labeling functions for  $s$ , thus by unicity  $t^{\mathcal{J}}(p) = t^{\mathcal{J}}(q)$ . Consequently, the set  $\{t^{\mathcal{J}}(p) \mid t|_p = s\}$  is a singleton (hence is finite). □

The converse of Proposition 16 does not hold (see Section 5). Note that the definition of  $[t]^{\mathcal{I}}$  that is given in Definition 15 coincides with the usual one if  $t$  is finite. A co-inductive interpretation associates a value to each (admissible) term, and a regularly co-inductive interpretation interprets only rational terms. We emphasize that a term may admit several labeling functions in a regularly co-inductive interpretation, provided exactly one of them is regular (see Section 5 for more details). Any interpretation  $\mathcal{I}$  on standard sorts can be extended into a regularly co-inductive interpretation by interpreting terms of a sort in  $\mathcal{S}_{\text{ci}}$  as rational terms defined on a signature containing all constructors and all elements of the domain of  $\mathcal{I}$ .

The truth value ( $\top$  or  $\perp$ ) of a formula  $\phi$  in an interpretation  $\mathcal{I}$  is denoted by  $[\phi]^{\mathcal{I}}$  and defined inductively as usual, with the proviso that rational formulas can be interpreted only in interpretations that are regularly co-inductive, and arbitrary (i.e., not necessarily rational) formulas can be interpreted only in co-inductive interpretations (finite formulas may be interpreted in all interpretations):



- If  $\phi = P(t_1, \dots, t_n)$  then  $[\phi]^{\mathcal{I}} = \top$  iff  $P^{\mathcal{I}}([t_1]^{\mathcal{I}}, \dots, [t_n]^{\mathcal{I}}) = \top$ .
- If  $\phi = (\phi_1 \vee \phi_2)$  then  $[\phi]^{\mathcal{I}} = \top$  iff  $[\phi_i]^{\mathcal{I}} = \top$ , for some  $i = 1, 2$ .
- If  $\phi = \neg\psi$  then  $[\phi]^{\mathcal{I}} = \top$  iff  $[\psi]^{\mathcal{J}} = \perp$ .
- If  $\phi = \exists x.\psi$  then  $[\phi]^{\mathcal{I}} = \top$  iff there exists a associate  $\mathcal{J}$  of  $\mathcal{I}$  that coincides with  $\mathcal{I}$  on all variables other than  $x$  such that  $[\psi]^{\mathcal{J}} = \top$ .

We write  $\mathcal{I} \models \phi$  if  $[\phi]^{\mathcal{J}} = \top$  for every associate  $\mathcal{J}$  of  $\mathcal{I}$ .

**Proposition 17.** *Let  $\mathcal{I}$  be a regularly co-inductive interpretation. For every rational term  $t = f(t_1, \dots, t_n)$  we have  $[t]^{\mathcal{I}} = f^{\mathcal{I}}([t_1]^{\mathcal{I}}, \dots, [t_n]^{\mathcal{I}})$ .*

*Proof.* By definition,  $[t]^{\mathcal{I}} = \mu(\varepsilon)$  where  $\mu$  is the regular labeling function for  $t$ . By Condition 2 in Definition 11, we deduce  $[t]^{\mathcal{I}} = f^{\mathcal{I}}(\mu(1), \dots, \mu(n))$ . Moreover, by Proposition 13,  $\mu|_i$  is a regular labeling function for  $t_i$ , thus  $\mu(i) = \mu|_i(\varepsilon) = [t_i]^{\mathcal{I}}$ . Hence  $[t]^{\mathcal{I}} = f^{\mathcal{I}}([t_1]^{\mathcal{I}}, \dots, [t_n]^{\mathcal{I}})$ .  $\square$

### 3 Axiomatization

We devise a finite axiomatization of regularly co-inductive interpretations, thus reducing the problem of determining whether a formula admits a regularly co-inductive model to a standard satisfiability test in first-order logic.

#### 3.1 New Symbols

The signature is extended as follows. We assume that the sets  $\mathcal{S}_{\text{sr}}$  and  $\Sigma$  contain the following symbols, not occurring in the initial formula:

- two standard sort symbols **nat** and **pos** that are meant to denote natural numbers and positions, respectively.
- two standard function symbols  $e : \rightarrow \text{pos}$  and  $\cdot : \text{nat}, \text{pos} \rightarrow \text{pos}$  that are meant to denote the empty position and the cons operation of positions, respectively.
- one predicate symbol  $\ll : \text{pos}, \text{pos} \rightarrow \text{bool}$ , denoting the (strict) length order on positions, and one constant symbol **i** for every  $i \in \{1, \dots, N\}$ , with  $N = \max\{\#(c) \mid c \in \mathcal{C}\}$ .
- two predicate symbols  $E_{\mathbf{s}} : \mathbf{s}, \mathbf{s} \rightarrow \text{bool}$  and  $C_{\mathbf{s}} : \mathbf{s}, \mathbf{s}, \text{pos} \rightarrow \text{bool}$  for every sort  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ .  $E_{\mathbf{s}}(x, y)$  states that  $x$  and  $y$  share the same head constructor symbol and the same set of non co-inductive arguments, and  $C_{\mathbf{s}}(x, y, z)$  states that  $x$  and  $y$  are not bisimilar, i.e., that  $\neg E_{\mathbf{t}}(x', y')$  holds for terms  $x', y'$  of sort  $\mathbf{t}$  occurring at position  $z$  in  $x$  and  $y$ , respectively.
- one sort symbol  $\tilde{\mathbf{s}} \in \mathcal{S}_{\text{sr}}$  and two functions  $\lambda_{\mathbf{s}} : \text{pos} \rightarrow \tilde{\mathbf{s}}$  and  $\tau_{\mathbf{s}} : \mathbf{s} \rightarrow \tilde{\mathbf{s}}$  for every sort symbol  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ , and one function  $\tilde{c} : \tilde{\mathbf{s}}_1, \dots, \tilde{\mathbf{s}}_m, \mathbf{s}_{m+1}, \dots, \mathbf{s}_n \rightarrow \tilde{\mathbf{s}}$  for all  $c : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s} \in \mathcal{C}$ , with  $m = \#_{\text{ci}}(c)$ . Following a similar approach as in [6], these function symbols will be used to encode constructor contexts. The term  $\lambda(p)$  denotes a “link” to the position  $p$ . Intuitively,  $\lambda(p)$  will be eventually interpreted as the term occurring at

position  $p$  in the considered context, which will allow us to encode infinite terms. The term  $\tau(x)$  will denote a trivial constructor context that is constantly identical to  $x$ . Let  $\tilde{\mathcal{S}}_{\text{ci}} = \{\tilde{\mathbf{s}} \mid \mathbf{s} \in \mathcal{S}_{\text{ci}}\}$ . For instance, the term  $\tilde{c}(\lambda(\varepsilon), \tilde{c}(\lambda(\varepsilon), \tau(y)))$  will denote a context of the form  $c(x, c(x, y))$ , where  $x$  is linked to the root of the term.

- a predicate symbol  $S_{\mathbf{s}, \mathbf{t}} : \mathbf{s}, \mathbf{t}, \text{pos} \rightarrow \text{bool}$  for each pair of sorts  $\{\mathbf{s}, \mathbf{t}\} \subseteq \mathcal{S}_{\text{ci}} \cup \tilde{\mathcal{S}}_{\text{ci}}$ , that is meant to denote the subterm relation, restricted to terms of a sort in  $\mathcal{S}_{\text{ci}} \cup \tilde{\mathcal{S}}_{\text{ci}}$  (i.e.,  $S_{\mathbf{s}, \mathbf{t}}(x, y, z)$  holds iff  $y$  is a subterm of sort  $\mathbf{t}$  occurring at position  $z$  in  $x$ ).
- one predicate symbol  $V_{\mathbf{s}} : \tilde{\mathbf{s}}, \mathbf{s} \rightarrow \text{bool}$ , for all  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ . Intuitively,  $V(x, y)$  states that  $y$  is the value of the constructor term encoded by  $x$ , where every occurrence of  $\lambda$  is interpreted arbitrarily (the interpretation of  $\lambda$  will be specified later, see Axiom 13 below). For instance, the atom  $V(\tilde{c}(\lambda(\varepsilon), \tilde{c}(\lambda(\varepsilon), \tau(y))), c(x_1, c(x_2, y)))$  will hold, regardless of the value of  $x_1$  and  $x_2$ .

The symbols  $\cdot$  and  $\ll$  are written in infix notation. The symbols  $\tilde{c}$  with  $c \in \mathcal{C}$  will sometimes be called “constructors”, although their co-domain is not in  $\mathcal{S}_{\text{ci}}$ . As for  $\approx$ , the indices  $\mathbf{s}, \mathbf{t}$  in the above symbols will often be omitted, since they can be recovered from the arguments. Let  $\Omega$  be the set of symbols defined as follows:

$$\Omega \stackrel{\text{def}}{=} \{\text{nat}, \text{pos}, e, \cdot, \lambda_{\mathbf{s}}, \tau_{\mathbf{s}}, \tilde{\mathbf{s}}, \tilde{c}, \dot{\mathbf{i}}, \ll, S_{\mathbf{s}, \mathbf{t}}, E_{\mathbf{s}}, C_{\mathbf{s}}, V_{\mathbf{s}} \mid \mathbf{s}, \mathbf{t} \in \mathcal{S}_{\text{ci}}, 1 \leq i \leq N, c \in \mathcal{C}\}$$

A term or a formula is  $\Omega$ -independent if it contains no symbol in  $\Omega$  and no term of a sort in  $\Omega$ .

## 3.2 Axioms

We denote by  $\mathcal{A}$  the set of all formulas induced by schemata (1)-(14) below. Free variables are implicitly universally quantified, and empty disjunctions and conjunctions are always false and true, respectively. Axiom 1 states that the constructors are injective.

$$c(x_1, \dots, x_n) \approx c(y_1, \dots, y_n) \Rightarrow \bigwedge_{i=1}^n x_i \approx y_i \quad (1)$$

for all constructors  $c : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$ , where  $x_i, y_i$  ( $1 \leq i \leq n$ ) are pairwise distinct variables of sort  $\mathbf{s}_i$ .

Axiom 2 states that the range of the constructors are pairwise disjoint:

$$c(x_1, \dots, x_n) \not\approx d(y_1, \dots, y_m) \quad (2)$$

for all sorts  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$  and for all distinct constructors  $c : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$ ,  $d : \mathbf{t}_1, \dots, \mathbf{t}_m \rightarrow \mathbf{s}$ , where  $x_i$  ( $1 \leq i \leq n$ ) and  $y_j$  ( $1 \leq j \leq m$ ) are pairwise distinct variables of sort  $\mathbf{s}_i$  and  $\mathbf{t}_j$ .

Axiom 3 states that all the elements of the domain of a co-inductive sort are in the range of some constructor.

$$\bigvee_{c: \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s} \in \mathcal{C}} \exists x_1^c \dots \exists x_n^c. x \approx c(x_1^c, \dots, x_n^c) \quad (3)$$

for all  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ , where  $x$  denotes a variable of sort  $\mathbf{s}$  and  $x_i^c$  are pairwise distinct variables of sort  $\mathbf{s}_i$ , also distinct from  $x$ .

Axiom 4 states that a position is either of the form  $e$  or  $\mathbf{i} \cdot y$ , for some  $i = 1, \dots, N$  and Axiom 5 states that the cons operator on positions is injective ( $x, y$  are distinct variables of sort  $\mathbf{pos}$ ).

$$x \approx e \vee \bigvee_{i=1}^N \exists y. x \approx \mathbf{i} \cdot y \quad (4)$$

$$\mathbf{j} \cdot x \not\approx \mathbf{k} \cdot y \wedge (\mathbf{j} \cdot x \approx \mathbf{j} \cdot y \Rightarrow x \approx y) \quad (\text{for all distinct numbers } j, k \text{ in } \{1, \dots, N\}) \quad (5)$$

Note that the axiom  $e \not\approx \mathbf{i} \cdot x$  is not needed<sup>2</sup>.

Axioms 6 and 7 define the semantics of  $S(x, y, z)$ , by induction on  $z$  ( $i$  ranges over  $\{1, \dots, \#_{\text{ci}}(c)\}$  in Axiom 7 because we only consider subterms of a sort in  $\mathcal{S}_{\text{ci}}$ ).

$$S(x, y, e) \Leftrightarrow x \approx y \quad (6)$$

for all sorts  $\mathbf{s} \in \mathcal{S}_{\text{ci}} \cup \tilde{\mathcal{S}}_{\text{ci}}$ , where  $x, y$  are distinct variables of sort  $\mathbf{s}$ .

$$z \not\approx e \Rightarrow \left( S(c(x_1, \dots, x_n), y, z) \Leftrightarrow \bigvee_{i=1}^{\#_{\text{ci}}(c)} \exists w. (z \approx \mathbf{i} \cdot w \wedge S(x_i, y, w)) \right) \quad (7)$$

for all sorts  $\mathbf{s}, \mathbf{t} \in \mathcal{S}_{\text{ci}} \cup \tilde{\mathcal{S}}_{\text{ci}}$  and for all constructors  $c : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$ , where  $x_1, \dots, x_n, y, z, w$  are pairwise distinct variables of sort  $\mathbf{s}_1, \dots, \mathbf{s}_n, \mathbf{t}, \mathbf{pos}, \mathbf{pos}$ , respectively.

Axiom 8 defines the semantics of  $\ll$ . The symbols  $x, y, z, w$  are pairwise distinct variables of sort  $\mathbf{pos}$ .

$$x \ll y \Leftrightarrow \exists z. \exists w. \bigvee_{i=1}^N \left( y \approx \mathbf{i} \cdot z \wedge (x \approx z \vee x \ll z \vee \bigvee_{j=1}^N (x \approx \mathbf{j} \cdot w \wedge w \ll z)) \right) \quad (8)$$

Intuitively,  $x \ll y$  holds when  $x$  and  $y$  are of the form  $\mathbf{i}_1 \cdot \dots \cdot \mathbf{i}_n \cdot x'$  and  $\mathbf{j}_1 \cdot \dots \cdot \mathbf{j}_m \cdot x'$ , respectively, with  $m > n$ . This axiom may seem a bit peculiar, as we assume that  $x$  and  $y$  end with the same arbitrary position  $x'$  rather than with the empty position  $\varepsilon$ . This is required because non standard interpretations exist, where positions are not interpreted as finite sequences. Consequently, one cannot assume that all positions end with  $\varepsilon$ , and using a base case such that  $x \approx \varepsilon \wedge y \not\approx \varepsilon$  would not be sufficient (see Examples 19 and 20).

Axioms 9 and 10 define the semantics of  $E$  and  $C$ , respectively<sup>3</sup>.

<sup>2</sup>Intuitively, positions are mainly used for defining the subterm relation  $S$ . The semantics of  $S(x, y, e)$  is defined by Axiom 6 and Axiom 7 covers the inductive case. Since the latter formula takes  $z \not\approx e$  as an hypothesis, there cannot be any overlap between these two axioms.

<sup>3</sup>Note that it is not useful to specify the semantics of  $E(x, y)$  when  $x, y$  have distinct heads, although we could assume that  $E(x, y)$  is false in this case. Indeed  $\neg E(x, y)$  will be used only to prove that  $x \not\approx y$  holds, but if  $x$  and  $y$  have distinct constructor heads, then the result is immediate by Axiom 2.

$$E(c(x_1, \dots, x_n), c(y_1, \dots, y_n)) \Leftrightarrow \bigwedge_{i=1+\#_{\text{ci}}(c)}^n (x_i \approx y_i) \quad (9)$$

for all  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$  and for all constructors  $c : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$ , where  $x_i, y_i$  are pairwise distinct variables of sort  $\mathbf{s}_i$  (for  $i = 1, \dots, n$ ).

$$C(x, y, z) \Leftrightarrow \bigvee_{\mathbf{t} \in \mathcal{S}_{\text{ci}}} \exists x_{\mathbf{t}}, \exists y_{\mathbf{t}}. (S(x, x_{\mathbf{t}}, z) \wedge S(y, y_{\mathbf{t}}, z) \wedge \neg E(x_{\mathbf{t}}, y_{\mathbf{t}})) \quad (10)$$

for every  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ , where  $z$  is a variable of sort  $\text{pos}$ ,  $x, y$  are pairwise distinct variables of sort  $\mathbf{s}$  and  $x_{\mathbf{t}}, y_{\mathbf{t}}$  are pairwise distinct variables of sort  $\mathbf{t}$ , also distinct from  $x, y$ .

Note that the subterms  $x_i, y_i$  of a sort in  $\mathcal{S}_{\text{ci}}$  are not taken into account in Axiom 9. For instance, if  $c$  is a constructor of profile  $\mathbf{t} \rightarrow \mathbf{s}$  with  $\mathbf{s}, \mathbf{t} \in \mathcal{S}_{\text{ci}}$ , and  $\zeta_i = c^{\mathcal{I}}(\xi_i)$  (for all  $i = 1, 2$ ), for some interpretation  $\mathcal{I}$  and elements  $\zeta_1, \zeta_2, \xi_1, \xi_2$  then  $E^{\mathcal{I}}(\zeta_1, \zeta_2)$  is true, regardless of the value of  $\xi_1$  and  $\xi_2$ . Omitting co-inductive arguments is essential to ensure that  $C$  properly axiomatizes non bisimilarity. For instance, assume that  $d : \mathbf{s} \rightarrow \mathbf{s}$  is a constructor (with  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ ) and consider an interpretation  $\mathcal{I}$  with two distinct elements  $\zeta'_1, \zeta'_2$  such that  $\zeta'_i = d^{\mathcal{I}}(\zeta'_i)$  (for all  $i = 1, 2$ ). If co-inductive arguments were to be considered in Axiom 9 then  $E^{\mathcal{I}}(\zeta'_1, \zeta'_2)$  would be equivalent to  $\zeta'_1 \approx \zeta'_2$ , hence would be false, thus  $C^{\mathcal{I}}(\zeta'_1, \zeta'_2, e)$  would be true (by Axiom 10). However, it is clear that  $\zeta'_1$  and  $\zeta'_2$  are bisimilar.

Axiom 11 states that  $C(x, y, z)$  holds only if  $x$  and  $y$  are distinct.

$$C(x, y, z) \Rightarrow x \not\approx y \quad (11)$$

for all  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ , where  $z$  is a variable of sort  $\text{pos}$ ,  $x, y$  are pairwise distinct variables of sort  $\mathbf{s}$ .

Axiom 12 gives the semantics of  $V$ , i.e., defines a mapping from the terms encoding constructor contexts to terms in the initial signature:

$$\begin{aligned} V(x, y) \Leftrightarrow \exists z. (x \approx \lambda(z)) \vee x \approx \tau(y) \vee \\ \left( \bigvee_{c: \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s} \in \mathcal{C}} \exists x_1^c, \dots, x_n^c, y_1^c, \dots, y_n^c. (x \approx \tilde{c}(x_1^c, \dots, x_n^c) \wedge y \approx c(y_1^c, \dots, y_n^c)) \right. \\ \left. \wedge \bigwedge_{i=1}^{\#_{\text{ci}}(c)} V(x_i^c, y_i^c) \wedge \bigwedge_{i=\#_{\text{ci}}(c)+1}^n x_i^c \approx y_i^c) \right) \quad (12) \end{aligned}$$

for all sorts  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ , where  $x, y, z$  are pairwise distinct variables of sorts  $\tilde{\mathbf{s}}, \mathbf{s}$  and  $\text{pos}$ , and for all  $c : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$ ,  $x_i^c, y_i^c$  ( $1 \leq i \leq n$ ) are pairwise distinct variables (also distinct from  $x, y$ ),  $y_i^c$  is of sort  $\mathbf{s}_i$  and  $x_i^c$  is of sort  $\tilde{\mathbf{s}}_i$  if  $i \leq \#_{\text{ci}}(c)$  and  $\mathbf{s}_i$  otherwise.

Note that  $V(\lambda(x), y)$  always holds. The link to the position denoted by  $x$  is expressed by Axiom 13. This axiom states that every infinite term has a value. To this aim, we assert that all constructor contexts have a value  $y$  in which

every occurrence of  $\lambda(z)$  is interpreted as the term at position  $z$  in  $y$ :

$$\exists y. V(x, y) \wedge \bigwedge_{\mathfrak{t} \in \mathcal{S}_{\text{ct}}} \forall z \forall w \forall x_{\mathfrak{t}} \forall y_{\mathfrak{t}} \forall y'_{\mathfrak{t}}. (S(x, \lambda(z), w) \wedge S(y, y_{\mathfrak{t}}, z) \wedge S(x, x_{\mathfrak{t}}, z) \wedge S(y, y'_{\mathfrak{t}}, w) \Rightarrow y_{\mathfrak{t}} \approx y'_{\mathfrak{t}}) \quad (13)$$

for all  $\mathfrak{s} \in \mathcal{S}_{\text{ct}}$ , where  $x$  and  $y$  are of sort  $\tilde{\mathfrak{s}}$  and  $\mathfrak{s}$ , respectively,  $z, w$  are distinct variables of sort  $\text{pos}$ ,  $x_{\mathfrak{t}}$  is a variable of sort  $\tilde{\mathfrak{t}}$ , distinct from  $x$ , and  $y_{\mathfrak{t}}, y'_{\mathfrak{t}}$  are distinct variables of sort  $\mathfrak{t}$ , also distinct from  $y$ .

The atom  $S(x, x_{\mathfrak{t}}, z)$  may seem redundant, but it is useful to ensure that  $z$  is a finite position (see the proof of Theorem 26 for more details).

Finally, Axiom 14 states that distinct terms  $x, y$  of the same sort cannot be bisimilar, which is expressed by asserting that there exists a position  $z$  such that  $C(x, y, z)$  holds. We also assert that this position is a minimal one with respect to the order  $\ll$ . This will allow us to simulate a form of inductive reasoning (see Example 20 below and the proof of Theorem 30).

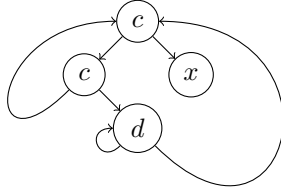
$$x \not\approx y \Rightarrow \exists z. (C(x, y, z) \wedge \forall z'. (z' \ll z \Rightarrow \neg C(x, y, z')) \quad (14)$$

for all  $\mathfrak{s} \in \mathcal{S}_{\text{ct}}$ , where  $x, y$  are pairwise distinct variables of sort  $\mathfrak{s}$ ,  $z, z'$  are pairwise distinct variables of sort  $\text{pos}$ .

### 3.3 Examples

Before establishing the soundness and completeness of the axiomatization, we provide examples of application. We first show how Axiom 13 can be used to assert that a rational term has a value.

**Example 18.** Let  $c, d$  be constructors of profile  $\mathfrak{s}, \mathfrak{s} \rightarrow \mathfrak{s}$ . Let  $t = c(c(t, s), x)$  be an infinite term, with  $s = d(s, t)$ . This term is depicted graphically as follows:



Let  $t'$  be the finite term of sort  $\tilde{\mathfrak{s}}$ :  $t' = \tilde{c}(\tilde{c}(\lambda(e), \tilde{d}(\lambda(p), \lambda(e))), \tau(x))$ , with  $p = 1 \cdot 2 \cdot e$ . The term  $t'$  can be viewed as a representation of the infinite term  $t$ , where the subterms  $\lambda(e)$  and  $\lambda(p)$  correspond to links to the subterms at positions  $\varepsilon$  and  $1.2$ , respectively. These links are intended to denote “loops” inside the term. Let  $\zeta' = [t']^{\mathcal{I}}$ . By Axiom 13, if  $\mathcal{I}$  is a model of  $\mathcal{A}$ , then there exists an element  $\zeta$  such that  $V^{\mathcal{I}}(\zeta', \zeta)$  is true. By (several applications of) Axiom 12, this entails that  $\zeta$  is of the form  $c^{\mathcal{I}}(c^{\mathcal{I}}(\zeta_1, d^{\mathcal{I}}(\zeta_2, \zeta_3)), x^{\mathcal{I}})$ , for some elements  $\zeta_1, \zeta_2$  and  $\zeta_3$ . Let  $z = 1.1.e$ . By Axioms 6 and 7,  $S^{\mathcal{I}}(\zeta', \lambda(e), z^{\mathcal{I}})$ ,  $S^{\mathcal{I}}(\zeta, \zeta, e^{\mathcal{I}})$ ,  $S^{\mathcal{I}}(\zeta', \zeta', e^{\mathcal{I}})$  and  $S^{\mathcal{I}}(\zeta, \zeta_1, z^{\mathcal{I}})$  must be true thus  $\zeta = \zeta_1$  (by the second part of Axiom 13). Similarly, by letting  $z = 1.2.1.e$  and  $z = 1.2.2.e$ , respectively, we get  $\zeta|_{1.2} = \zeta_2$

and  $\zeta = \zeta_3$ . This entails that  $\zeta$  is a possible interpretation of the infinite term  $t$ .

As shown in the proof of Lemma 29, the same idea can be applied to any rational term. Next, we show how Axiom 14 can be used to assert that two bisimilar terms are equal.

**Example 19.** Let  $t = c(t)$  be an infinite term. Let  $\mathcal{I}$  be a model of  $\mathcal{A}$  and assume that there exist two distinct elements  $\zeta_1, \zeta_2$  such that  $\zeta_i = c^{\mathcal{I}}(\zeta_i)$  (for  $i = 1, 2$ ), yielding two different values for the term  $t$ . By Axiom 14, as by hypothesis  $\zeta_1 \neq \zeta_2$ , there exists a minimal (w.r.t.  $\ll^{\mathcal{I}}$ ) element  $\xi$  of sort **pos** such that  $C^{\mathcal{I}}(\zeta_1, \zeta_2, \xi)$  holds. By Axiom 10, this entails that there exist  $\zeta'_i$  such that  $S^{\mathcal{I}}(\zeta_i, \xi, \zeta'_i)$  is true (for all  $i = 1, 2$ ) and  $E^{\mathcal{I}}(\zeta'_1, \zeta'_2)$  is false. We exploit the fact that  $\xi$  is minimal w.r.t.  $\ll^{\mathcal{I}}$  to derive a contradiction. This effectively simulates an application of the induction principle on the set of positions:

- If  $\xi = e^{\mathcal{I}}$ , then, using Axiom 6, we get  $\zeta_i = \zeta'_i$  (for all  $i = 1, 2$ ). Thus  $E^{\mathcal{I}}(\zeta_1, \zeta_2)$  is false, which contradicts Axiom 9 (as  $\zeta_1$  and  $\zeta_2$  have the same constructor head  $c$  and no non co-inductive argument).
- Otherwise, by Axiom 4,  $\xi$  must be of the form  $\mathbf{i} \cdot^{\mathcal{I}} \xi'$ , and by Axioms 5 and 7, necessarily  $\mathbf{i} = 1$  and  $S^{\mathcal{I}}(\zeta_i, \xi', \zeta'_i)$  must be true (as by hypothesis  $\zeta_i = c^{\mathcal{I}}(\zeta_i)$ ). Thus  $C^{\mathcal{I}}(\zeta_1, \zeta_2, \xi')$  is true, which contradicts the minimality of  $\xi$ , as (by Axiom 8)  $\xi' \ll^{\mathcal{I}} \xi$ .

The same idea is used in Lemma 28 to show that every rational term admits at most one regular labeling function. We provide another example, that is similar but slightly more complex.

**Example 20.** We show how the equation  $a \approx b$  may be derived from  $a \approx c(a, b)$  and  $b \approx c(b, a)$  using the above axioms (if  $c$  is a constructor). Assume that  $a \approx b$  does not hold. From Axiom 14, we deduce that there exists a  $\ll$ -minimal element  $p$  such that  $C(a, b, p)$  holds. By Axiom 10, this entails that there exist  $x, y$  such that  $S(a, x, p)$  and  $S(b, y, p)$  hold and  $E(x, y)$  does not hold. If  $p \approx e$  holds then we get (using Axiom 6)  $x \approx a \approx c(a, b)$  and  $y \approx b \approx c(b, a)$  thus  $\neg E(c(a, b), c(b, a))$  which contradicts Axiom 9 (since  $\#_{\mathbf{c}_1}(c) = 2$ ). Therefore  $p \not\approx e$  holds and (by Axiom 4)  $p$  is of the form  $\mathbf{i} \cdot q$  (for  $i \in \{1, \dots, N\}$ ). Note that by Axiom 8,  $q \ll p$  holds. By Axioms 5 and 7, we have either  $i = 1$  or  $i = 2$ , and we derive (using the equations  $a \approx c(a, b)$  and  $b \approx c(b, a)$ ): either  $S(a, x, q)$  and  $S(b, y, q)$ , or  $S(b, x, q)$  and  $S(a, y, q)$ . By Axiom 10, this entails in both cases that  $C(a, b, q)$  is true, which contradicts the minimality of  $p$ .

### 3.4 Soundness and Refutational Completeness

We now prove that the proposed axiomatization is sound and complete w.r.t. regularly co-inductive interpretations, in the sense that a formula admits a regularly co-inductive model iff it admits a model in which all the above axioms are true. Since all co-inductive interpretations are also regularly co-inductive, the axiomatization is also sound for co-inductive interpretations, but it is not complete w.r.t. those: if  $\mathcal{A} \cup \{\phi\}$  is unsatisfiable then  $\phi$  admits no regularly co-inductive interpretation (hence no co-inductive interpretation), and if  $\mathcal{A} \cup \{\phi\}$  is satisfiable, then  $\phi$  admits a regularly co-inductive interpretation, that is possibly not co-inductive.

We first extend the notations  $t(p)$  and  $t|_p$  to elements of the domain of an interpretation:

**Definition 21.** For every interpretation  $\mathcal{I}$  satisfying Axioms 1 and 2, and for every element  $\zeta$  in the domain of  $\mathcal{I}$ ,  $\zeta|_p$  is inductively defined as follows:  $\zeta|_\varepsilon \stackrel{\text{def}}{=} \zeta$ ,  $\zeta|_{i.p} \stackrel{\text{def}}{=} \xi$ , iff  $\zeta = c^{\mathcal{I}}(\zeta_1, \dots, \zeta_n)$  with  $c \in \mathcal{C}$ ,  $\xi = \zeta_i|_p$  and  $i = 1, \dots, n$ . Note that  $\xi$  is well-defined since  $c$  is unique (by Axiom 2) and  $c^{\mathcal{I}}$  is injective (by Axiom 1), however the function  $p \mapsto \zeta|_p$  is partial. We write  $\zeta(p) = c$  if  $\zeta|_p$  is of the form  $c^{\mathcal{I}}(\zeta_1, \dots, \zeta_n)$ . Note that this entails that  $\zeta|_p$  is of a sort in  $\mathcal{S}_{c_i}$ . We denote by  $\text{dom}(\zeta)$  the set of positions such that  $\zeta(p)$  is defined. An element  $\zeta$  is rational if the set of elements of the form  $\zeta|_p$  is finite. We write  $\zeta \cong \zeta'$  if  $\zeta$  and  $\zeta'$  are bisimilar, i.e.,  $\text{dom}(\zeta) = \text{dom}(\zeta')$  and for every position  $p \in \text{dom}(\zeta)$ :  $\zeta(p) = \zeta'(p)$  and  $\#_{c_i}(\zeta(p)) < i \leq \#(\zeta(p)) \implies \zeta|_{p.i} = \zeta'|_{p.i}$ .

**Proposition 22.** Let  $\mathcal{I}$  be an interpretation satisfying Axioms 1 and 2, and let  $\zeta$  be an element of the domain of  $\mathcal{I}$ . If  $\zeta(p) = c$  then  $\zeta|_p = c^{\mathcal{I}}(\zeta|_{p.1}, \dots, \zeta|_{p.n})$ .

*Proof.* The proof follows immediately from Definition 21.  $\square$

**Proposition 23.** Let  $\mathcal{I}$  be a regularly co-inductive interpretation. Let  $t$  be a term and let  $p \in \text{dom}(t)$ .  $[t]^{\mathcal{I}}|_p = [t|_p]^{\mathcal{I}}$ .

*Proof.* The proof is by an immediate induction on  $p$  (using Proposition 17).  $\square$

**Proposition 24.** If  $\mathcal{I}$  satisfies Axioms 1, 2 and 3 then for every element  $\zeta$  of the domain of  $\mathcal{I}$ :  $p \in \text{dom}(\zeta)$  iff  $\zeta|_p$  is defined and of a sort in  $\mathcal{S}_{c_i}$ .

*Proof.* This is immediate, since Axiom 3 entails that  $\zeta|_p$  (if defined) must be of the form  $c^{\mathcal{I}}(\zeta_1, \dots, \zeta_n)$  for some  $c \in \mathcal{C}$ , thus  $\zeta(p) = c$ .  $\square$

We first prove that the axiomatization is sound. We need the following lemma:

**Lemma 25.** Let  $\mathcal{I}$  be an interpretation and let  $\zeta, \zeta'$  be distinct elements of the domain of  $\mathcal{I}$ . Assume that the set  $\{\zeta|_p \mid p \in P\}$  with  $P = \{p \mid p \in \text{dom}(\zeta) \wedge (p \notin \text{dom}(\zeta') \vee \zeta|_p \neq \zeta'|_p)\}$  is infinite. There exists an infinite branch  $\pi$  such that, for every position  $p \prec \pi$ :  $p \in P$ , and  $|q| \geq |p|$  holds for all positions  $q$  such that  $\zeta|_q = \zeta|_p$  and  $\zeta'|_q = \zeta'|_p$ . Such a branch is called direct (for the pair  $(\zeta, \zeta')$ ).

*Proof.* Note that  $P$  is closed under prefix. We first construct infinite sequences of positions  $p_0 \prec p_2 \prec \dots$  and of infinite sets  $\Gamma_0 \supseteq \Gamma_2 \supseteq \dots$  of elements of the domain of  $\mathcal{I}$ , in such a way that the following invariant  $(\star)$  is satisfied, for every  $j \geq 0$ : for every  $\xi \in \Gamma_j$ , there exists a position  $q(j, \xi)$  such that  $p_j.q(j, \xi) \in P$ ,  $\zeta|_{p_j.q(j, \xi)} = \xi$ , and  $|r| \geq |p_j| + |q(j, \xi)|$  holds for all positions  $r \in P$  such that  $\zeta|_r = \xi$ . Initially,  $p_0 \stackrel{\text{def}}{=} \varepsilon$ ,  $\Gamma_j$  is the set of elements  $\xi$  such that  $\xi = \zeta|_q$  for some position  $q \in P$ , and  $q(0, \xi)$  is any position of minimal length in  $P$  such that  $\zeta|_{q(0, \xi)} = \xi$ . It is clear that  $\star$  is satisfied for  $j = 0$ . Now, assume that  $p_j$  and  $\Gamma_j$  have been constructed and that  $\star$  holds for  $j$ . By definition, each position in  $q(j, \xi)$  (with  $\xi \in \Gamma_j$ ) is either  $\varepsilon$  or of the form  $i.q'(j, \xi)$ , for some  $i \in \{1 \dots N\}$  and position  $q'(j, \xi)$ . For every  $i = 1, \dots, N$ , we denote by  $\Gamma_j^i$  the set of elements  $\xi \in \Gamma_j$  such that  $q(j, \xi) = i.q'(j, \xi)$ . Since  $\Gamma_j$  is infinite, there exists  $i \in \{1, \dots, N\}$  such that  $\Gamma_j^i$  is infinite. We define:  $p_{j+1} \stackrel{\text{def}}{=} p_j.i$ ,  $\Gamma_{j+1} \stackrel{\text{def}}{=} \Gamma_j^i$  and  $q(j+1, \xi) \stackrel{\text{def}}{=} q'(j, \xi)$ , for all  $\xi \in \Gamma_j^i$ . We now show

that property  $\star$  holds for  $j + 1$ . Let  $\xi \in \Gamma_{j+1}$ . Since  $\Gamma_{j+1} = \Gamma_j^i \subseteq \Gamma_j$ , we have  $\xi \in \Gamma_j$  hence by the induction hypothesis we get  $\zeta|_{p_j \cdot q(j, \xi)} = \xi$ ,  $p_j \cdot q(j, \xi) \in P$  and  $\forall r \in P : \zeta|_r = \xi \implies |r| \geq |p_j| + |q(j, \xi)|$ . By definition,  $p_{j+1} = p_j \cdot i$ ,  $q(j, \xi) = i \cdot q'(j, \xi)$  and  $q(j+1, \xi) \stackrel{\text{def}}{=} q'(j, \xi)$ , thus we get  $\zeta|_{p_{j+1} \cdot i \cdot q'(j, \xi)} = \xi$ , i.e.,  $\zeta|_{p_{j+1} \cdot q(j+1, \xi)} = \xi$ , with  $p_{j+1} \cdot q(j+1, \xi) \in P$ , and  $\forall r \in P : \zeta|_r = \xi \implies |r| \geq |p_{j+1}| - 1 + |q'(j, \xi)| + 1 = |p_{j+1}| + |q'(j, \xi)| = |p_{j+1}| + |q(j+1, \xi)|$ . Thus  $\star$  holds.

Now consider the infinite branch  $\pi$  such that  $p_j \prec \pi$ , for all  $j \geq 0$  (such a branch exists since  $p_j \prec p_{j+1}$ , for all  $j \geq 0$ ). Note that we must have  $p_j \in P$ , for all  $j \in \mathbb{N}$  (otherwise we cannot have  $p_j \cdot q(j, \xi) \in P$  for any  $\xi \in \Gamma_j$ ). Assume that there exist positions  $p \prec \pi$  and  $q$  such that  $\xi = \zeta|_p = \zeta|_q$ ,  $\zeta'|_p = \zeta'|_q$  and  $|q| < |p|$ . By definition,  $p = p_j$ , for some  $j \geq 0$ . Consider any element  $\chi \in \Gamma_j$ . By  $\star$ , we have  $\zeta|_{p_j \cdot q(j, \chi)} = \chi$ , thus, since  $\zeta|_{p_j} = \xi$ , we get  $\xi|_{q(j, \chi)} = \chi$ , and using the fact that  $\xi = \zeta|_q$ , we deduce:  $\zeta|_{q \cdot q(j, \chi)} = \chi$ . Moreover  $q \cdot q(j, \chi) \in P$ , as  $p_j \cdot q(j, \chi) \in P$ , with  $\zeta|_{p_j} = \zeta|_q$ ,  $\zeta'|_{p_j} = \zeta'|_q$ . Since  $\chi \in \Gamma_j$ , this entails (by  $\star$ ) that  $|q \cdot q(j, \chi)| \geq |p_j| + |q(j, \chi)|$ , i.e.,  $|q| \geq |p_j|$ , which contradicts our assumption.  $\square$

**Theorem 26.** (*Soundness*) *For every  $\Omega$ -independent rational formula  $\phi$ , if  $\phi$  admits a regularly co-inductive model, then the set  $\{\phi\} \cup \mathcal{A}$  is satisfiable.*

*Proof.* We show that every regularly co-inductive model of  $\phi$  may be extended into a model of the above axioms. The proof is more involved than expected, because interpreting the symbols in a “canonical” way (following the explanations given above) is actually not sufficient. The positions and the subterm relation must be interpreted in a non standard way. Indeed, to satisfy Axiom 14, we must ensure that for all distinct elements  $\zeta, \zeta'$ , there exists a position  $p$  such that  $\zeta$  and  $\zeta'$  differ at  $p$ . But finite positions satisfying this property do not always exist, as the considered interpretation is not necessarily co-inductive:  $\zeta$  and  $\zeta'$  may be bisimilar and distinct. As we will see, this is possible only if at least one of the elements  $\zeta, \zeta'$  is rational, as otherwise  $\mathcal{I}$  cannot be regularly co-inductive. To overcome this issue, we add (for all bisimilar elements  $\zeta, \zeta'$  such that  $\zeta$  or  $\zeta'$  is not rational) a special position  $p$  in the domain, and we assert that the subterms occurring at  $p$  in  $\zeta$  and  $\zeta'$  are  $\kappa_0$  and  $\kappa_1$ , respectively, where  $\kappa_0$  and  $\kappa_1$  are arbitrary elements with distinct constructor heads. This special position will be defined as a tuple  $(0, \varepsilon, \zeta, \zeta')$ . To understand the rôle of the first two components, one needs to keep in mind that all the other axioms must be fulfilled as well, in particular Axioms 4 and 7. By Axiom 4, the position  $(0, \varepsilon, \zeta, \zeta')$  must correspond to some branch  $\pi = (i_1, \dots, i_n, \dots)$  in both  $\zeta$  and  $\zeta'$ , and by Axiom 7,  $\kappa_0$  and  $\kappa_1$  must be subterms of  $\zeta|_{i_1, \dots, i_n}$  and  $\zeta'|_{i_1, \dots, i_n}$  (for all  $n \in \mathbb{N}$ ). The branch  $\pi$  must be infinite, as  $\zeta, \zeta'$  are bisimilar. We will denote by  $(n, \varepsilon, \zeta, \zeta')$  the position of  $\kappa_0$  and  $\kappa_1$  in  $\zeta|_{i_1, \dots, i_n}$  and  $\zeta'|_{i_1, \dots, i_n}$  respectively, and we shall define the cons operation on positions in such a way that  $i_{n+1} \cdot (n+1, \varepsilon, \zeta, \zeta') = (n, \varepsilon, \zeta, \zeta')$ . We also define the relation  $S^{\mathcal{J}}$  in such a way that  $\kappa_0$  and  $\kappa_1$  occur in  $\zeta|_{i_1, \dots, i_n}$  and  $\zeta'|_{i_1, \dots, i_n}$  at position  $(0, \varepsilon, \zeta, \zeta')$ . However, this is not sufficient to fulfill the axioms, as the cons operation must be defined also for positions outside of the branch  $\pi$ , e.g., for the positions  $i \cdot (n+1, \varepsilon, \zeta, \zeta')$ , with  $i \neq i_{n+1}$ . To overcome this issue, we will make use of the second component and define  $i \cdot (n, \varepsilon, \zeta, \zeta')$  as  $(n, i, \zeta, \zeta')$ , if  $i \neq i_{n+1}$ . Similarly,  $i \cdot (n, p, \zeta, \zeta')$  will be defined as  $(n, i, p, \zeta, \zeta')$ , if  $p \neq \varepsilon$ . The definition of  $S^{\mathcal{J}}$  can be adapted to take these cases into account. Finally, we must also ensure that the position  $p$  is minimal. This is here where Lemma 25 comes into play. It ensures (assuming



that one of the elements, say  $\zeta$ , is not rational) that the branch  $\pi$  can be chosen in such a way that it is direct for  $(\zeta, \zeta')$ , so that, for all  $n$ ,  $i_1 \dots i_n$  is a minimal position of  $\zeta|_{i_1 \dots i_n}$  and  $\zeta'|_{i_1 \dots i_n}$  in  $\zeta, \zeta'$ , respectively. As we shall see, this property entails that  $p$  is indeed minimal w.r.t.  $\ll^{\mathcal{I}}$ .

Let  $\mathcal{I}$  be a regularly co-inductive model of  $\phi$ . We construct a model  $\mathcal{J}$  of  $\{\phi\} \cup \mathcal{A}$  as follows.  $\mathcal{I}$  and  $\mathcal{J}$  coincide on all symbols not occurring in  $\Omega$ . This entails that  $\mathcal{J} \models \phi$ , since  $\phi$  is  $\Omega$ -independent (hence by definition contains no symbol in  $\Omega$ ). Let  $\kappa_0$  and  $\kappa_1$  be arbitrary domain elements of the same sort occurring in the range of distinct constructors<sup>4</sup>. Let  $\mathfrak{S}$  be the set of ordered pairs  $(\zeta, \xi)$  satisfying the following properties:  $\zeta \neq \xi$ ,  $\text{dom}(\zeta) = \text{dom}(\xi)$ ,  $\zeta(p) = \xi(p)$  for all  $p \in \text{dom}(\zeta)$  and  $(\zeta, \zeta')$  admits a direct infinite branch  $\pi(\zeta, \zeta')$  (if several direct infinite branches in  $\zeta$  exist then  $\pi(\zeta, \zeta')$  denotes one of them, chosen arbitrarily). We denote by  $\pi(\zeta, \zeta')_i$  the  $i$ -th number in the (infinite) sequence  $\pi(\zeta, \zeta')$  (starting at 1, i.e.,  $\pi(\zeta, \zeta')_0$  is undefined). Note that by Conditions 1, 2 and 3 in Definition 14 (respectively), Axioms 1, 2 and 3 necessarily hold in  $\mathcal{I}$ , hence in  $\mathcal{J}$ . We then fix the interpretation of the symbols in  $\Omega$ .

- $\text{nat}^{\mathcal{J}} \stackrel{\text{def}}{=} \{1, \dots, N\}$ , with  $i^{\mathcal{I}} \stackrel{\text{def}}{=} i$ .
- $\text{pos}^{\mathcal{J}}$  contains all positions as well as all tuples of the form  $(i, p, \zeta, \xi)$  where  $p$  is a position,  $(\zeta, \xi) \in \mathfrak{S}$  and  $i \in \mathbb{N}$ . Intuitively,  $(0, \varepsilon, \zeta, \xi)$  will denote the minimal position at which  $\zeta$  and  $\xi$  differ.
- $e^{\mathcal{J}} \stackrel{\text{def}}{=} \varepsilon$ .
- For all  $i = 1 \dots, N$ ,  $(i \cdot^{\mathcal{J}} p) \stackrel{\text{def}}{=} i.p$  if  $p$  is a position, and if  $p = (j, q, \zeta, \xi)$  then  $(i \cdot^{\mathcal{J}} p) \stackrel{\text{def}}{=} (j-1, q, \zeta, \xi)$  if  $q = \varepsilon$ ,  $j > 0$  and  $\pi(\zeta, \zeta')_j = i$ , and otherwise  $(i \cdot^{\mathcal{J}} p) \stackrel{\text{def}}{=} (j, i.q, \zeta, \xi)$ . The cons operation  $\cdot^{\mathcal{J}}$  may be extended to the case where the left operand is a finite position by an immediate induction.
- $p \ll^{\mathcal{J}} q \iff \exists p', i_1, \dots, i_n, j_1, \dots, j_m \text{ s.t. } m > n, p = i_1 \cdot^{\mathcal{J}} \dots i_n \cdot^{\mathcal{J}} p' \text{ and } q = j_1 \cdot^{\mathcal{J}} \dots j_m \cdot^{\mathcal{J}} p'$ .
- $\tilde{\mathfrak{s}}^{\mathcal{J}}$  is the set of finite terms built on the signature containing all the symbols in  $\tilde{\mathcal{C}}$ , the symbols  $\lambda$  and  $\tau$ , all elements in  $\text{pos}^{\mathcal{J}}$  and all elements in some set  $\mathfrak{t}^{\mathcal{I}}$  with  $\mathfrak{t} \notin \tilde{\mathcal{S}}_{\text{ci}}$  (viewed as constants of sort  $\mathfrak{t}$ ). Every  $n$ -ary function symbol  $f \in \{\tilde{c}, \lambda, \tau \mid c \in \mathcal{C}\}$  is interpreted as the mapping:  $x_1, \dots, x_n \mapsto f(x_1, \dots, x_n)$ .
- $S^{\mathcal{J}}(\chi, \rho, p)$  is true iff  $p$  is a position and  $\chi|_p = \rho$ , or if  $p = q \cdot^{\mathcal{J}}(i, \varepsilon, \zeta, \xi)$  with  $(\zeta, \xi) \in \mathfrak{S}$ ,  $r \prec \pi(\zeta, \zeta')$ ,  $i = |r|$ , and either  $\rho = \kappa_0$  and  $\chi|_q = \zeta|_r$  or  $\rho = \kappa_1$  and  $\chi|_q = \xi|_r$ .
- $V^{\mathcal{J}}(\zeta, \xi)$  is true iff  $\zeta$  is of the form  $\lambda(p)$ , or  $\zeta = \tau(\xi)$ , or there exists a constructor  $c$  such that  $\zeta = \tilde{c}(\zeta_1, \dots, \zeta_n)$ ,  $\xi = c^{\mathcal{J}}(\xi_1, \dots, \xi_n)$ ,  $\zeta_i = \xi_i$  for all  $i = \#_{\text{ci}}(c) + 1, \dots, n$  and  $V^{\mathcal{J}}(\zeta_i, \xi_i)$  for all  $i = 1, \dots, \#_{\text{ci}}(c)$  (the definition is well-founded since  $\zeta_i$  and  $\xi_i$  are finite terms and  $\text{size}(\zeta_i) < \text{size}(\zeta)$ ). We remind that the size of a rational term is the number of pairwise distinct subterms occurring in it.

<sup>4</sup>Such elements exist since we assumed that there is least one sort  $\mathfrak{s} \in \mathcal{S}_{\text{ci}}$  with two distinct constructors of co-domain  $\mathfrak{s}$ .

- $E^{\mathcal{I}}(\zeta, \xi)$  is true iff there exists a constructor  $c$  such that  $\zeta = c^{\mathcal{I}}(\zeta_1, \dots, \zeta_n)$ ,  $\xi = c^{\mathcal{I}}(\xi_1, \dots, \xi_n)$  and  $\zeta_i = \xi_i$  for  $i = \#_{\text{ct}}(c) + 1, \dots, n$ .
- $C^{\mathcal{I}}(\zeta, \xi, p)$  is true iff there exist  $\zeta', \xi'$  such that  $S^{\mathcal{I}}(\zeta, \zeta', p)$ ,  $S^{\mathcal{I}}(\xi, \xi', p)$  are true and  $E^{\mathcal{I}}(\zeta', \xi')$  is false.

For instance, assume that the signature contains a constructor  $c : \mathbf{s} \rightarrow \mathbf{s}$ , with  $\mathbf{s}^{\mathcal{I}} = \mathbb{Z}$  and  $c^{\mathcal{I}}(x) \stackrel{\text{def}}{=} x + 1$ . Then 0 and 1 (as all elements  $i, j \in \mathbb{Z}$ ) are bisimilar. The branch  $\pi(0, 1)$  is  $1 \dots 1 \dots$ . Then the tuple  $(0, \varepsilon, 0, 1)$  denotes the special position at which 0 and 1 differ, and  $S^{\mathcal{I}}(0, (0, \varepsilon, 0, 1), \kappa_0)$ ,  $S^{\mathcal{I}}(1, (0, \varepsilon, 0, 1), \kappa_1)$  are true. As  $-1 = 0|_1$  and  $0 = 1|_1$ ,  $S^{\mathcal{I}}(-1, (1, \varepsilon, 0, 1), \kappa_0)$  and  $S^{\mathcal{I}}(0, (1, \varepsilon, 0, 1), \kappa_1)$  and also true, and, more generally,  $S^{\mathcal{I}}(-i, (i, \varepsilon, 0, 1), \kappa_0)$  and  $S^{\mathcal{I}}(1-i, (i, \varepsilon, 0, 1), \kappa_1)$  are true. We have  $(0, \varepsilon, 0, 1) = 1 \cdot^{\mathcal{J}}(1, \varepsilon, 0, 1) = 1 \cdot^{\mathcal{J}} 1 \cdot^{\mathcal{J}}(2, \varepsilon, 0, 1) = \dots = 1^n \cdot^{\mathcal{J}}(n, \varepsilon, 0, 1)$ , for all  $n \in \mathbb{N}$ . Furthermore,  $1 \cdot^{\mathcal{J}}(0, \varepsilon, 0, 1) = (0, 1, 0, 1)$  and  $2 \cdot^{\mathcal{J}}(1, \varepsilon, 0, 1) = (1, 2, 0, 1)$ ,  $3 \cdot^{\mathcal{J}} 2 \cdot^{\mathcal{J}}(1, \varepsilon, 0, 1) = (1, 3, 2, 0, 1)$ , etc. Now, consider an element  $\xi = d^{\mathcal{I}}(-1, -1)$ , where  $d : \mathbf{s}, \mathbf{s} \rightarrow \mathbf{s}$  is a constructor. We have  $-1 = \xi|_1 = \xi|_2$ , thus  $S^{\mathcal{I}}(\xi, (0, \varepsilon, 0, 1), \kappa_0)$  and  $S^{\mathcal{I}}(\xi, (1, 2, 0, 1), \kappa_0)$  hold.

From the above definition, it is straightforward to check that Axioms 4, 5, 6, 8, 9, 10, 12 hold. We now check that Axioms 7, 11, 13 and 14 hold.

7 Let  $\zeta = c^{\mathcal{J}}(\zeta_1, \dots, \zeta_n)$ , and assume that  $\chi \neq e^{\mathcal{J}}$ , i.e.,  $\chi \neq \varepsilon$ .

- Assume that  $S^{\mathcal{J}}(\zeta, \xi, \chi)$  is true. If  $\chi$  is a finite position then by definition of  $S^{\mathcal{J}}$  we get  $\zeta|_{\chi} = \xi$ , so that  $\chi$  must be of the form  $i \cdot \rho$  with  $i \in \{1, \dots, n\}$  and  $\zeta_i|_{\rho} = \xi$ , hence  $S^{\mathcal{J}}(\zeta_i, \xi, \rho)$  is true (since  $\rho$  is also finite). Assume that  $\chi$  is a tuple  $q \cdot^{\mathcal{J}}(i, \varepsilon, \zeta', \xi')$ . Then we get  $\xi = \kappa_0$  and  $\zeta|_q = \zeta'|_r$  or  $\xi = \kappa_1$  and  $\zeta|_q = \xi'|_r$  with  $i = |r|$ ,  $r \prec \pi(\zeta', \xi')$ . Assume by symmetry that the first disjunct holds. Let  $j = \pi(\zeta', \xi')_{i+1}$ . By definition (since  $|r| = i$ ), we have  $r \cdot j \prec \pi(\zeta', \xi')$  and  $\zeta|_{q \cdot j} = \zeta'|_{r \cdot j}$ . If  $q = \varepsilon$ , then let  $\rho' = (i+1, \varepsilon, \zeta', \xi')$ . By definition of  $\cdot^{\mathcal{J}}$ , we have  $j \cdot^{\mathcal{J}} \rho' = (i, \varepsilon, \zeta', \xi') = \rho$ , and by definition of  $S^{\mathcal{J}}$ ,  $S^{\mathcal{J}}(\zeta_i, \xi, \rho')$  is true (since  $|r \cdot j| = i+1$ ). Otherwise, we have  $q = k \cdot q'$ , with  $\zeta_k|_{q'} = \zeta'|_r$ . Let  $\rho'' = q' \cdot^{\mathcal{J}}(i, \varepsilon, \zeta', \xi')$ , we have  $\rho = j \cdot^{\mathcal{J}} \rho''$ . By definition of  $S^{\mathcal{J}}$ ,  $S^{\mathcal{J}}(\zeta_k, \xi, \rho'')$  is true.
- Now, assume that  $S^{\mathcal{J}}(\zeta_j, \xi, \rho)$  holds, and that  $\chi = j \cdot^{\mathcal{J}} \rho$ . If  $\rho$  is a finite position then we get  $\zeta_j|_{\rho} = \xi$ , so that  $\zeta|_{\chi} = \xi$ , and thus  $S^{\mathcal{J}}(\zeta, \xi, \chi)$  is true. Otherwise,  $\rho = q \cdot^{\mathcal{J}}(i, \varepsilon, \zeta', \xi')$ . Then we get either  $\xi = \kappa_0$  and  $\zeta_j|_q = \zeta'|_r$  or  $\xi = \kappa_1$  and  $\zeta_j|_q = \xi'|_r$  with  $i = |r|$  and  $r \prec \pi(\zeta', \xi')$ . Moreover,  $\zeta_j|_q = \zeta|_{j \cdot q}$  and  $\chi = j \cdot q \cdot^{\mathcal{J}}(i, \varepsilon, \zeta', \xi')$ . Thus  $S^{\mathcal{J}}(\zeta, \xi, \chi)$  is true.

- 11 Assume that there exist  $\zeta, \xi$  such that  $C^{\mathcal{J}}(\zeta, \zeta, \xi)$  holds. This entails that there exist  $\chi, \rho$  such that  $E^{\mathcal{J}}(\chi, \rho)$  is false and both  $S^{\mathcal{J}}(\zeta, \chi, \xi)$  and  $S^{\mathcal{J}}(\zeta, \rho, \xi)$  are true. Using the fact that  $E^{\mathcal{J}}(\chi, \rho)$  is false and Axioms 3, 9, 2 and 1, it is easy to show that  $\chi \neq \rho$ . If  $\xi$  is a finite position, then by definition of  $S^{\mathcal{J}}$  we have  $\zeta|_{\xi} = \chi$  and  $\zeta|_{\xi} = \rho$ , which contradicts the fact that  $\chi \neq \rho$ . Otherwise, we must have  $\{\chi, \rho\} = \{\kappa_0, \kappa_1\}$  (by definition of  $S^{\mathcal{J}}$ ) and  $\xi$  is necessarily of the form  $(i, p, \zeta', \xi')$  with  $(\zeta', \xi') \in \mathfrak{S}$ . By definition of  $S^{\mathcal{J}}$ , we have  $\zeta|_p = \zeta'|_r = \xi'|_r$ , with  $|r| = i$ , which contradicts the fact that  $\pi(\zeta', \xi')$  is direct.

13: Consider any sort  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$  and any element  $t$  in  $\tilde{\mathbf{s}}^{\mathcal{J}}$ . By definition,  $t$  is a finite term built on the signature described above. We assume that for every element  $\zeta \in \mathfrak{t}^{\mathcal{I}}$  with  $\mathfrak{t} \notin \tilde{\mathcal{S}}_{\text{ci}}$  occurring in  $t$  there exists a variable  $x$  such that  $x^{\mathcal{I}} = \zeta$  (this is without loss of generality since there are finitely many such elements  $\zeta$  and there always exists some associate of  $\mathcal{I}$  such that the property holds). We define a function  $\omega(\cdot)$  mapping every subterm  $s$  of  $t$  to an infinite term, defined as follows.

- (a) If  $s = \tilde{c}(s_1, \dots, s_n)$  then  $\omega(s) \stackrel{\text{def}}{=} c(\omega(s_1), \dots, \omega(s_n))$ .
- (b) If  $s = \lambda_{\mathbf{s}}(p)$ , then  $\omega(s) \stackrel{\text{def}}{=} \omega(t|_p)$  if  $t(p)$  is a constructor of co-domain  $\mathbf{s}$ , otherwise  $\omega(s)$  is defined arbitrarily.
- (c) If  $s = \tau(u)$  then  $\omega(s) = x$ , where  $x^{\mathcal{I}} = u$ .
- (d) Otherwise,  $\omega(s) = x$ , where  $x^{\mathcal{I}} = s$ .

Note that  $\omega(s)$  is well-defined, since the symbol occurring at root position in  $\omega(s)$  is set by the above definition, either immediately, or, in the second case, at the next recursive call. Thus every position in the term is eventually defined. Furthermore, by definition every subterm of  $\omega(t)$  is of the form  $\omega(s)$  for some subterm  $s$  of  $t$ , hence  $\omega(t)$  is necessarily rational, since  $t$  is finite. Note that for every constructor position  $p$  in  $t$ , we have  $\omega(t)|_p = \omega(t|_p)$  (this follows from the first item above by an immediate induction on  $p$ ).

Let  $\zeta = [\omega(t)]^{\mathcal{I}}$ . It is straightforward to verify (by an easy induction on  $t$ ) that  $V^{\mathcal{J}}(t, \zeta)$  is true. Furthermore, if  $S^{\mathcal{J}}(t, \lambda(p), q)$ ,  $S^{\mathcal{J}}(\zeta, \chi, p)$ ,  $S^{\mathcal{J}}(t, \rho, p)$  and  $S^{\mathcal{J}}(\zeta, \chi', q)$  are true, then by definition of  $S^{\mathcal{J}}$ , necessarily  $p$  and  $q$  must be finite constructor positions in  $t$ , and we must have  $t|_q = \lambda(p)$ ,  $\rho = t|_p$ ,  $\chi' = \zeta|_q$  and  $\chi = \zeta|_p$ . By Proposition 23, we get:  $\chi = [\omega(t)]^{\mathcal{I}}|_p = [\omega(t)|_p]^{\mathcal{I}} = [\omega(t|_p)]^{\mathcal{I}}$ . By definition of the function  $\omega(\cdot)$ , necessarily  $\omega(\lambda(p)) = \omega(t|_p)$ , and using again Proposition 23, we obtain:  $\zeta|_q = [\omega(t)]^{\mathcal{I}}|_q = [\omega(t)|_q]^{\mathcal{I}} = [\omega(t|_q)]^{\mathcal{I}} = [\omega(\lambda(p))]^{\mathcal{I}} = [\omega(t|_p)]^{\mathcal{I}} = \zeta|_p$ . Hence  $\chi = \chi'$ . Thus Axiom 13 is satisfied.

14: Let  $\zeta, \xi$  be distinct elements of some sort  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ . We have to prove that there exists a  $\ll^{\mathcal{J}}$ -minimal element  $\chi$  such that  $C^{\mathcal{J}}(\zeta, \xi, \chi)$  is true. If there exists a finite position  $p \in \text{dom}(\zeta) \cap \text{dom}(\xi)$  such that  $E^{\mathcal{J}}(\zeta|_p, \xi|_p)$  is false, then it suffices to define  $\chi$  as the length-minimal position  $p$  such that  $E^{\mathcal{J}}(\zeta|_p, \xi|_p)$  is false. Since tuples cannot be lower than  $p$  w.r.t.  $\ll^{\mathcal{I}}$ , it is clear that  $\chi$  is indeed minimal. Now, assume that no such position exists. We prove that  $\text{dom}(\zeta) = \text{dom}(\xi)$ . By symmetry, we only have to check that  $\text{dom}(\zeta) \subseteq \text{dom}(\xi)$ . Assume the contrary, and let  $p$  be a position of minimal length such that  $p \in \text{dom}(\zeta)$  and  $p \notin \text{dom}(\xi)$ . By Proposition 24, Axiom 3, since  $\zeta$  and  $\xi$  are of a sort in  $\mathcal{S}_{\text{ci}}$ , necessarily  $\varepsilon \in \text{dom}(\zeta) \cap \text{dom}(\xi)$ , hence  $p \neq \varepsilon$ . Consequently,  $p = q.i$ , and by minimality of  $p$ ,  $q \in \text{dom}(\zeta) \cap \text{dom}(\xi)$ . Moreover, by the assertion above we have  $\zeta(q) = \xi(q)$ , thus  $\zeta|_q$  and  $\xi|_q$  must be of the form  $c(\zeta_1, \dots, \zeta_n)$  and  $c(\xi_1, \dots, \xi_n)$ , for some  $c \in \mathcal{C}$ . Since  $q.i \in \text{dom}(\zeta)$ ,  $\zeta|_p$  is defined, hence  $i \in \{1, \dots, n\}$ , thus  $\xi|_p$  must be defined. Moreover,  $\zeta|_p$  and  $\xi|_p$  are of the same sort, which entails by Proposition 24 that  $p \in \text{dom}(\xi)$ , contradicting our hypothesis. Thus  $\text{dom}(\zeta) = \text{dom}(\xi)$ , and for every position  $p \in \text{dom}(\zeta)$ :  $\zeta(p) = \xi(p)$ .

Consider the term  $t$  defined as follows:

- if  $p \in \text{dom}(\zeta)$  then  $t(p) \stackrel{\text{def}}{=} \zeta(p)$ ,
- if  $\zeta|_p = c(\zeta_1, \dots, \zeta_n)$ , with  $c : \mathfrak{s}_1, \dots, \mathfrak{s}_n \rightarrow \mathfrak{s}$ ,  $i = 1, \dots, n$  and  $p.i \notin \text{dom}(p)$  then  $t(p.i) = x_{\zeta,i}$ , where  $x_{\zeta,i}$  denote pairwise distinct variables of sort  $\mathfrak{s}_i$ , with  $x_{\zeta,i}^{\mathcal{J}} = \zeta|_{p.i}$ .

It is easy to check that  $t$  is a well-founded term and that the functions:  $t^{\mathcal{K}}$  and  $t^{\mathcal{L}}$  such that  $t^{\mathcal{K}}(p) = \zeta|_p$  and  $t^{\mathcal{L}}(p) = \xi|_p$  satisfy Conditions 1 and 2 in Definition 11. If both  $\zeta$  and  $\xi$  are rational, then necessarily  $t$  is rational and the sets  $\{\zeta|_p, p \in \text{dom}(t)\}$  and  $\{\xi|_p \mid p \in \text{dom}(t)\}$  are both finite. In this case, Condition 3 is also satisfied, and  $t^{\mathcal{K}}$  and  $t^{\mathcal{L}}$  are regular labeling functions for  $t$ . By unicity of the regular labeling function (Definition 15), we deduce that  $t^{\mathcal{K}}(\varepsilon) = t^{\mathcal{L}}(\varepsilon)$ , thus  $\zeta = \xi$ . Otherwise, one of the elements  $\zeta$  or  $\xi$  is irrational. Assume by symmetry that  $\zeta$  is irrational. By definition, as  $\zeta \neq \xi$ , and  $\zeta$  and  $\xi$  are bisimilar, the set  $\{\zeta|_p \mid p \in \mathbb{N}^*, \zeta|_p \neq \xi|_p\}$  is also infinite. By Lemma 25 the pair  $(\zeta, \xi)$  admits a direct branch  $\pi(\zeta, \xi)$ , which entails that  $(\zeta, \xi) \in \mathfrak{S}$ . By definition  $S^{\mathcal{J}}(\zeta, \kappa_0, (0, \varepsilon, \zeta, \xi))$  and  $S^{\mathcal{J}}(\xi, \kappa_1, (0, \varepsilon, \zeta, \xi))$  are both true. Since, by definition of  $\kappa_0, \kappa_1$ ,  $E^{\mathcal{J}}(\kappa_0, \kappa_1)$  is false, this entails that  $C^{\mathcal{J}}(\zeta, \xi, (0, \varepsilon, \zeta, \xi))$  is true. Now assume that  $C^{\mathcal{J}}(\zeta, \xi, \chi)$  holds, for some position  $\chi$  such that  $\chi \ll^{\mathcal{J}} (0, \varepsilon, \zeta, \xi)$ . Then  $\chi$  must be of the form  $q \cdot^{\mathcal{J}}(i, \varepsilon, \zeta, \xi)$ , with  $i \in \mathbb{N}$  and  $|q| < i$ , and  $(0, \varepsilon, \zeta, \xi) = r \cdot^{\mathcal{J}}(i, \varepsilon, \zeta, \xi)$  with  $r \prec \pi(\zeta, \xi)$  and  $|r| = i$ . Since  $\pi(\zeta, \xi)$  is direct, we have  $\zeta|_r \neq \xi|_r$ . By Axiom 10,  $S^{\mathcal{J}}(\zeta, \kappa_0, \chi)$  and  $S^{\mathcal{J}}(\xi, \kappa_1, \chi)$  must be true. This entails that  $\zeta|_q = \zeta|_r$  and  $\xi|_q = \xi|_r$ , and since  $\pi(\zeta, \xi)$  is direct, we deduce that  $|q| \geq |r| = i$ , which contradicts the previous assertion. Hence Axiom 14 is satisfied.  $\square$

We now prove that the axiomatization is complete. To this purpose, we show that every model of  $\mathcal{A}$  is regularly co-inductive. The proof is decomposed into several lemmata.

**Lemma 27.** *Every interpretation satisfying Axioms 1, 2 and 3 is  $\mathcal{C}$ -normal.*

*Proof.* Conditions 1, 2 and 3 in Definition 14 stem immediately from Axioms 1, 2 and 3 respectively.  $\square$

**Lemma 28.** *Let  $\mathcal{I}$  be a  $\mathcal{C}$ -normal interpretation satisfying Axioms 4, 5, 6, 7, 8, 9, 10, 11 and 14. Every rational term  $t$  admits at most one regular labeling function w.r.t.  $\mathcal{I}$ .*

*Proof.* Assume that there exist a rational term  $t$  and two distinct functions  $\mu$  and  $\nu$  satisfying Conditions 1, 2 and 3 in Definition 11. Let  $p$  be a position such that  $\mu(p) \neq \nu(p)$ . Since  $t$  is rational, we may assume, w.l.o.g., that  $p$  is chosen in such a way that  $\text{size}(t|_p)$  is minimal. If  $t(p)$  is a variable  $x$ , then by Condition 1, we get  $\mu(p) = x^{\mathcal{I}}$  and  $\nu(p) = x^{\mathcal{I}}$ , so that  $\mu(p) = \nu(p)$ , contradicting the above assumption. Thus  $\mu(p) \in \Sigma$ . Let  $f = \mu(p)$  and let  $k$  be the arity of  $f$ . By definition of a term, necessarily  $p.i \in \text{dom}(t)$ , for all  $i = 1, \dots, k$ .

Assume first that  $t|_p$  is not a proper subterm of itself. Then, we must have  $\text{size}(t|_{p.i}) < \text{size}(t|_p)$  for all  $i = 1, \dots, k$ . By minimality of  $\text{size}(t|_p)$ , we deduce that  $\mu(p.i) = \nu(p.i)$  holds for all  $i = 1, \dots, k$ . By Condition 2 in Definition 11,

we get  $\mu(p.i) = f^{\mathcal{I}}(\mu(p.1), \dots, \mu(p.k))$  and  $\nu(p.i) = f^{\mathcal{I}}(\nu(p.1), \dots, \nu(p.k))$ , so that  $\mu(p) = \nu(p)$ , which contradicts our assumption.

Consequently, we may assume that  $t|_p$  is a proper subterm of itself, i.e., there exists  $q$  such that  $t|_{p.q} = t|_p$ . Since  $t$  is admissible, the only symbols that can occur infinitely many times along a position in  $t$  are constructors, thus necessarily  $t(r) \in \mathcal{C}$  for all positions  $r$  such that  $t|_{p.q} = t|_p$  and  $p \preceq r \preceq q$ . Note that this entails that  $t|_p$  is of a sort in  $\mathcal{S}_{\text{ci}}$ . Let  $\zeta = \mu(p)$  and  $\zeta' = \nu(p)$ . Since  $\zeta \neq \zeta'$  and  $\zeta, \zeta'$  are of a sort in  $\mathcal{S}_{\text{ci}}$ , we deduce, using Axiom 14, that there exists an element  $\xi$  such that  $C^{\mathcal{I}}(\zeta, \zeta', \xi)$  is true and that  $C^{\mathcal{I}}(\zeta, \zeta', \xi')$  is false, for all  $\xi'$  such that  $\xi' \ll^{\mathcal{I}} \xi$ . Since  $C^{\mathcal{I}}(\zeta, \zeta', \xi)$  is true, using Axiom 10, we deduce that there exist  $\chi, \chi'$  such that  $S^{\mathcal{I}}(\zeta, \chi, \xi)$  and  $S^{\mathcal{I}}(\zeta', \chi', \xi)$  are true, and  $E^{\mathcal{I}}(\chi, \chi')$  is false. We now show, by induction on  $n$ , that for all  $n \geq 0$ , there exist  $\xi_n$  and a constructor position  $p_n = i_1 \dots i_n$  in  $\text{dom}(t|_p)$  such that  $\xi = \mathbf{i}_1^{\mathcal{I}} \cdot \dots \cdot \mathbf{i}_n^{\mathcal{I}} \cdot \xi_n$ ,  $S^{\mathcal{I}}(\mu(p.p_n), \chi, \xi_n)$  and  $S^{\mathcal{I}}(\nu(p.p_n), \chi', \xi_n)$  are true ( $\dagger$ ).

- The proof for  $n = 0$ , is immediate, by taking  $\xi_0 = \xi$  ( $p_0 = \varepsilon$  in this case).
- Assume that the property holds for some  $n \geq 0$ . If  $\xi_n = e^{\mathcal{I}}$ , then we get (using  $\dagger$  and Axiom 6) that  $\chi = \mu(p.p_n)$  and  $\chi' = \nu(p.p_n)$ . Since  $p.p_n$  is a constructor position, necessarily  $t(p.p_n) = c \in \mathcal{C}$ , thus we get (by Condition 2 in Definition 11):  $\mu(p.p_n) = c^{\mathcal{I}}(\mu(p.p_n.1), \dots, \mu(p.p_n.m))$  and  $\nu(p.p_n) = c^{\mathcal{I}}(\nu(p.p_n.1), \dots, \nu(p.p_n.m))$ , with  $m = \#(c)$ . Moreover, for all  $i > \#_{\text{ci}}(c)$ , we have  $\text{size}(t|_{p.p_n.i}) < \text{size}(t|_{p.p_n}) = \text{size}(t|_p)$  (since  $t|_{p.p_n.i}$  cannot be of a sort in  $\mathcal{S}_{\text{ci}}$  hence cannot occur infinitely often along some position in  $t$ ), thus (by minimality of  $\text{size}(t|_p)$ ) we deduce that  $\mu(p.p_n.i) = \nu(p.p_n.i)$ , for all  $i = \#_{\text{ci}}(c)+1, \dots, m$ . However, since  $E^{\mathcal{I}}(\mu(p.p_n), \nu(p.p_n))$  is false, this contradicts Axiom 9. Therefore,  $\xi_n \neq e^{\mathcal{I}}$ , hence by Axiom 4, we deduce that  $\xi_n = \mathbf{i}_{n+1}^{\mathcal{I}} \cdot \xi_{n+1}$ , for some  $i_{n+1} \leq N$ . Let  $p_{n+1} = i_1 \dots i_{n+1}$ . Using Assertions  $\dagger$  in the inductive hypothesis together with Axioms 4 and 7, we deduce that  $i_{n+1} \leq m$  and that  $S^{\mathcal{I}}(\mu(p.p_{n+1}), \chi, \xi_{n+1})$  and  $S^{\mathcal{I}}(\nu(p.p_{n+1}), \chi', \xi_{n+1})$  are true. By Axiom 10, this entails (using the fact that  $E^{\mathcal{I}}(\chi, \chi')$  is false) that  $C^{\mathcal{I}}(\mu(p.p_{n+1}), \nu(p.p_{n+1}), \xi_{n+1})$  is true. If  $t|_p$  does not occur in  $t|_{p.p_{n+1}}$  then we have, by minimality of  $\text{size}(t|_p)$ ,  $\mu(p.p_{n+1}) = \nu(p.p_{n+1})$ . Since  $C^{\mathcal{I}}(\mu(p.p_{n+1}), \nu(p.p_{n+1}), \xi_{n+1})$  is true, this contradicts Axiom 11. Thus  $t|_p$  must occur in  $t|_{p.p_{n+1}}$ , which entails that  $p_{n+1}$  is a constructor position.

Since the property holds for all  $n \geq 0$  necessarily  $t|_p$  occurs infinitely often in the sequence  $t|_{p.p_n}$ . By Condition 3, the sets  $\{\mu(p.p_n) \mid t|_{p.p_n} = t\}$  and  $\{\nu(p.p_n) \mid t|_{p.p_n} = t\}$  are both finite, thus the set of pairs  $\{(\mu(p.p_n), \nu(p.p_n)) \mid t|_{p.p_n} = t\}$  is also finite. Consequently, there exist numbers  $k < l$  such that  $\mu(p.p_k) = \mu(p.p_l)$ ,  $\nu(p.p_k) = \nu(p.p_l)$ , and  $t|_{p.p_k} = t|_{p.p_l} = t$ . By  $\dagger$ , we deduce that  $S(\mu(p.p_k), \chi, \xi_l)$  and  $S^{\mathcal{I}}(\nu(p.p_k), \chi', \xi_l)$  are true. Using Axiom 7, this entails that  $S^{\mathcal{I}}(\mu(p), \chi, \xi')$  and  $S^{\mathcal{I}}(\nu(p), \chi', \xi')$  are also true, with  $\xi' \stackrel{\text{def}}{=} \mathbf{i}_1 \dots \mathbf{i}_k \cdot \xi_l$  thus by Axiom 10,  $C^{\mathcal{I}}(\mu(p), \nu(p), \xi')$  must be true. However, since  $l > k$ , by Axiom 8, we have  $\xi' \ll^{\mathcal{I}} \xi = \mathbf{i}_1 \dots \mathbf{i}_l \cdot \xi_l$ , thus this contradicts the fact that  $\xi$  is a  $\ll^{\mathcal{J}}$ -minimal element such that  $C^{\mathcal{I}}(\zeta, \zeta', \xi)$  is true.  $\square$

**Lemma 29.** *Let  $\mathcal{I}$  be a  $\mathcal{C}$ -normal interpretation satisfying Axioms 4, 5, 6, 7, 8, 12 and 13. Every rational term  $t$  admits at least one regular labeling function  $t^{\mathcal{I}}$  w.r.t.  $\mathcal{I}$ .*

*Proof.* Let  $t$  be a term. The function  $t^{\mathcal{I}}$  is defined by associating  $t$  with a finite constructor context obtained by replacing the constructors  $c$  by  $\tilde{c}$ , the subterms  $u$  not containing  $t$  by  $\tau(u)$  and by replacing some subterms occurring along infinite branches by a link to a previous position (using the symbol  $\lambda$ ). Axiom 13 ensures that this constructor context can be mapped to an element of the domain satisfying all the required properties. More formally, we assume, w.l.o.g., that a regular labeling function  $u^{\mathcal{I}}$  exists for all terms  $u$  such that  $\text{size}(u) < \text{size}(t)$ . For every position  $p = i_1 \dots i_n$  we denote by  $\hat{p}$  the term  $i_1 \dots i_n \cdot e$ . We distinguish two cases.

- Assume first that  $t$  is not a proper subterm of  $t$ . If  $t$  is a variable  $x$  then  $\text{dom}(t) = \{\epsilon\}$  and the function  $t^{\mathcal{I}}$  can be straightforwardly defined as follows:  $t^{\mathcal{I}}(\epsilon) = x^{\mathcal{I}}$ . We thus assume that  $t$  is a compound term  $f(t_1, \dots, t_n)$ . Necessarily (since  $t$  is not a proper subterm of  $t$ ),  $t$  cannot occur in  $t_i$ , and  $\text{size}(t_i) < \text{size}(t)$  which entails that  $t_i$  admits a regular labeling function  $\mu_i$ . By definition, every position in  $\text{dom}(t)$  is either  $\epsilon$  or of the form  $i.p$ , with  $i = 1, \dots, n$  and  $p \in \text{dom}(t_i)$ . The function  $t^{\mathcal{I}}$  is then defined as follows:  $t^{\mathcal{I}}(\epsilon) \stackrel{\text{def}}{=} f^{\mathcal{I}}(\mu_1(\epsilon), \dots, \mu_n(\epsilon))$ , and  $t^{\mathcal{I}}(i.p) \stackrel{\text{def}}{=} \mu_i(p)$ , for all  $i = 1, \dots, n$  and  $p \in \text{dom}(t_i)$ . We check that the conditions of Definition 11 are satisfied:

- 1: By definition, if  $t|_q = x \in \mathcal{V}$ , then  $q \neq \epsilon$  (since  $t$  is not a variable), thus  $q = i.p$ , with  $i = 1, \dots, n$  and  $p \in \text{dom}(t_i)$ . Moreover,  $t_i|_p = x$ , hence, since  $\mu_i$  satisfies Condition 1, we get  $t_i|_p(p) = x^{\mathcal{I}}$ , so that  $t^{\mathcal{I}}(p) = x^{\mathcal{I}}$ .
- 2: Let  $q$  be a position in  $\text{dom}(t)$  such that  $t|_q = g$ , for some  $m$ -ary function symbol  $g$ . If  $q = \epsilon$  then  $g = f$  and, by definition of  $t^{\mathcal{I}}$ :  $t^{\mathcal{I}}(\epsilon) = f^{\mathcal{I}}(\mu_1(\epsilon), \dots, \mu_n(\epsilon)) = f^{\mathcal{I}}(t^{\mathcal{I}}(1), \dots, t^{\mathcal{I}}(n))$ . Otherwise,  $q = i.p$  with  $i = 1, \dots, n$  and  $p \in \text{dom}(t_i)$  hence since  $\mu_i$  satisfies Condition 2, we get  $\mu_i(p) = g^{\mathcal{I}}(\mu_i(p.1), \dots, \mu_i(p.m))$ . By definition of  $t^{\mathcal{I}}$ , this entails that  $t^{\mathcal{I}}(q) = g^{\mathcal{I}}(t^{\mathcal{I}}(q.1), \dots, t^{\mathcal{I}}(q.m))$ .
- 3: Let  $s$  be a term. Since every function  $\mu_i$  ( $i = 1, \dots, n$ ) fulfills Condition 3, the set  $\{\mu_i(p) \mid t_i|_p = s\}$  is finite, thus  $\{\mu_i(p) \mid t_i|_p = s, i = 1, \dots, n\}$  is also finite. By definition of  $t^{\mathcal{I}}$ , this entails that the set  $\{t^{\mathcal{I}}(i.p) \mid t_{i.p} = s, i = 1, \dots, n\}$  is finite, hence the set  $\{t^{\mathcal{I}}(q) \mid t|_q = s\}$  is also finite (since there is only one position  $q = \epsilon$  that is not of the form  $i.p$ ).

- Now, assume that  $t$  is a proper subterm of  $t$ . Since all terms are admissible, this entails that  $t$  is of a sort  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$  and has a constructor head. We denote by  $<_{\text{lex}}$  the lexicographic order on position. Note that  $p < q \implies p <_{\text{lex}} q$ . By the above assumption, all subterms  $s$  of  $t$  such that  $\text{size}(s) < \text{size}(t)$  admit a regular labeling function  $s^{\mathcal{I}}$ , thus may be associated with an interpretation  $[s]^{\mathcal{I}}$ . We assume that, for every such subterm  $s$ , there exists a variable  $x_s$  such that  $x_s^{\mathcal{I}} = [s]^{\mathcal{I}}$ . This does not entail any loss of generality since there are finitely many such terms, hence there exists an associate of  $\mathcal{I}$  satisfying the property (and coinciding with  $\mathcal{I}$  on all variables in  $t$ ). Let  $\tau$  be a function (implicitly depending on  $t$ ) mapping every position  $p \in \text{dom}(t)$  to a term, inductively defined as follows:

$$- \tau(p) \stackrel{\text{def}}{=} x_{t|_p} \text{ if } t|_p \text{ is of a sort in } \mathcal{S}_{\text{st}}.$$

- $\tau(p) \stackrel{\text{def}}{=} \tau(x_{t|_p})$  if  $t$  is not a subterm of  $t|_p$  and  $t|_p$  is of a sort in  $\mathcal{S}_{\text{cr}}$ .
- $\tau(p) \stackrel{\text{def}}{=} \tilde{c}(\tau(p.1), \dots, \tau(p.n))$  if  $t|_p = c(s_1, \dots, s_n)$  and there is no position  $q <_{\text{lex}} p$  such that  $t|_q = t|_p$ .
- $\tau(p) \stackrel{\text{def}}{=} \lambda(q)$  if the previous condition does not hold and  $q$  is the minimal (w.r.t.  $<_{\text{lex}}$ ) position such that  $t|_p = t|_q$ .

Let  $P$  be the set of positions such that  $\tau(p)$  is a term of some head  $\tilde{c}$ . By definition of  $\tau$ , it is clear that for every subterm  $t'$  of  $t$  that contains  $t$ ,  $P$  contains exactly one position  $p$  such that  $t|_p = t'$  (this position is the minimal one w.r.t.  $<_{\text{lex}}$ ).

Let  $s = \tau(\epsilon)$ . It is straightforward to check that  $s$  is well-typed. Moreover, since  $t$  is rational, necessarily  $s$  is finite. Indeed, by the pigeonhole argument, if an infinite branch exists in  $t$ , then necessarily there are two positions  $p$  and  $q$  such that  $t|_p = t|_q$  and  $p \prec q$ . This entails that  $p <_{\text{lex}} q$  so that  $\tau(q)$  is of the form  $\lambda(r)$  (for some position  $r \leq_{\text{lex}} p$ ). Consequently,  $s$  has a value in  $\mathcal{I}$ , and we may define:  $\zeta = [s]^\mathcal{I}$ . By using Axiom 13, we deduce that there exists an element  $\xi$  such that  $V^\mathcal{I}(\zeta, \xi)$  is true and for all positions  $p, q$ , and for all elements  $\xi', \xi'', \zeta'$ , if  $S^\mathcal{I}(\xi, \xi', \hat{p})$ ,  $S^\mathcal{I}(\xi, \xi'', \hat{q})$ ,  $S^\mathcal{I}(\zeta, \zeta', \hat{p})$ , and  $S^\mathcal{I}(\zeta, \lambda^\mathcal{I}(\hat{p}), \hat{q})$  are true, then  $\xi' = \xi''$ . By definition of  $s$ , this entails that for all positions  $p, q$  such that  $\text{size}(t|_p) = \text{size}(t)$  and  $t|_p = t|_q$ , we have  $\xi|_p = \xi|_q$  ( $\dagger$ ).

Since  $V^\mathcal{I}(\zeta, \xi)$  is true, it is easy to check, using Axiom 12, that for every position  $p \in P$ , we have  $p \in \text{dom}(\xi)$  and  $\xi(p) = t(p)$ , and that, if moreover  $p.i \in \text{dom}(t)$  and  $\text{size}(t|_{p.i}) < \text{size}(t)$ , then  $s|_{p.i}$  is either  $x_{t|_{p.i}}$  or  $\tau(x_{t|_{p.i}})$ , so that  $\xi|_{p.i} = x_{t|_{p.i}}^\mathcal{I} = [t|_{p.i}]^\mathcal{I}$  ( $\star$ ).

The function  $t^\mathcal{I}$  is defined as follows.

- if  $p = q.r$  where  $q$  is some prefix minimal position such that  $\text{size}(t|_q) < \text{size}(t)$ , then  $t^\mathcal{I}(p) \stackrel{\text{def}}{=} t|_q^\mathcal{I}(r)$ .
- Otherwise, we define  $t^\mathcal{I}(p) \stackrel{\text{def}}{=} \xi|_q$ , where  $q$  is the (unique) position in  $P$  such that  $t|_p = t|_q$ .

We check that Conditions 1, 2 and 3 are satisfied.

- 1 Assume that  $t|_p = x$ . Then  $\text{size}(t|_p) < \text{size}(t)$ , thus  $t^\mathcal{I}(p) = t|_q^\mathcal{I}(r)$  for some positions  $q, r$  such that  $p = q.r$ . Since  $t|_q(r) = x$  and  $t|_q^\mathcal{I}$  satisfies Condition 1, we deduce that  $t^\mathcal{I}(p) = x^\mathcal{I}$ .
- 2 Assume that  $t(p)$  is an  $n$ -ary function symbol  $f$ . If  $t|_p$  does not contain  $t$  then  $t^\mathcal{I}(p) = t|_q^\mathcal{I}(r)$ , with  $p = q.r$ . Moreover, none of the terms  $t|_{p.i}$  may contain  $t$ , thus  $t^\mathcal{I}(p.i) = t|_q^\mathcal{I}(r.i)$ . Since  $t|_q^\mathcal{I}$  satisfies Condition 2, we deduce that  $t^\mathcal{I}(p) = f^\mathcal{I}(t^\mathcal{I}(p.1), \dots, t^\mathcal{I}(p.n))$ . If  $t|_p$  contains  $t$  we have  $t^\mathcal{I}(p) = \xi|_q$ , where  $q$  is the  $<_{\text{lex}}$ -minimal position such that  $t|_q = t|_p$ . By Proposition 22, we deduce  $t^\mathcal{I}(p) = f^\mathcal{I}(\xi|_{q.1}, \dots, \xi|_{q.n})$ . Let  $i = 1, \dots, n$ . If  $\text{size}(t|_{p.i}) = \text{size}(t)$ , then  $t^\mathcal{I}(p.i) = \xi|_r$ , where  $r \in P$  and  $t|_r = t|_{p.i}$ . Moreover, by Property  $\dagger$  above we have  $\xi|_r = \xi|_{q.i}$  (since  $t|_r = t|_{p.i} = t|_{q.i}$ ), thus  $t^\mathcal{I}(p.i) = \xi|_{q.i}$ . If  $q.i \in P$ , then we have  $t^\mathcal{I}(q.i) = \xi|_{q.i}$ , hence  $t^\mathcal{I}(p.i) = \xi|_{q.i}$  (since  $t|_{q.i} = t|_{p.i}$ ). Otherwise, we have (by the property  $\star$  above)  $\xi|_{q.i} = [t|_{q.i}]^\mathcal{I} = [t|_{p.i}]^\mathcal{I} = t^\mathcal{I}(p.i)$ .

Consequently,  $t^{\mathcal{I}}(p) = f^{\mathcal{I}}(t^{\mathcal{I}}(p.1), \dots, t^{\mathcal{I}}(p.n))$ .

- 3** Let  $s$  be a term. Since every function  $t_q^{\mathcal{I}}$  fulfills Condition **3**, every set  $\{t_q^{\mathcal{I}}(r) \mid t|_{q.r} = s\}$  is finite. Furthermore, the set of the prefix minimal positions  $q$  in  $t$  such that  $t$  is not a subterm of  $t_q$  is also finite. Since  $P$  is finite, this entails that  $\{t^{\mathcal{I}}(p) \mid t|_p = s\}$  is finite. □

**Theorem 30.** (Completeness) *Every model of  $\mathcal{A}$  is regularly co-inductive.*

*Proof.* The proof follows from Lemmata **27**, **28** and **29**. □

### 3.5 Comparison with Fixpoint Axioms

We compare our approach with that of [6]. We remind that the structures considered in [6] are defined by the following axioms: exhaustiveness (every term must occur in the range of some constructor, identical to Axiom **3** in the present paper), distinctness (the ranges of the constructors are pairwise distinct, Axiom **2**), injectivity (every constructor is injective, Axiom **1**), existence and uniqueness of fixpoints, and infinity (the domain of every sort  $\mathbf{s}$  is infinite). This set of axioms is denoted by  $\mathcal{A}^*$  (we refer to [6] for formal definitions). Given an interpretation  $\mathcal{I}$ , the axioms for unicity and existence of fixpoints hold iff for every finite constructor term  $t$  distinct from  $x$ , the equation  $x \approx t$  has only one solution, i.e., for every associate  $\mathcal{J}$  of  $\mathcal{I}$  there exists a unique element  $\zeta$  such that  $\zeta = [t]^{\mathcal{J}\{x \leftarrow \zeta\}}$ , where  $\mathcal{J}\{x \leftarrow \zeta\}$  denotes the associate of  $\mathcal{I}$  with  $x^{\mathcal{J}\{x \leftarrow \zeta\}} = \zeta$  and  $y^{\mathcal{J}\{x \leftarrow \zeta\}} = y^{\mathcal{I}}$  for all  $y \neq x$ . We may assume, w.l.o.g., that the only subterms occurring in  $t$  and not containing  $x$  are variables (since any such term can be replaced by a fresh variable interpreted in the same way).

It is clear that regularly co-inductive interpretations satisfy all these axioms, except (possibly) the infinity axiom. The infinity axiom is not necessary satisfied: if for instance  $\mathcal{C}$  contains a unique constructor  $c : \mathbf{s} \rightarrow \mathbf{s}$ , then there exists only one term, namely the infinite term  $t = c(t)$ , and the domain of  $\mathbf{s}$  is necessarily of cardinality 1. However the infinity axiom is satisfied under some rather natural conditions on the signature:

**Definition 31.** *A signature  $\Sigma$  is non trivial if for all  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ , there exist two constructors  $c, d$  of co-domain  $\mathbf{s}$ , with  $\#_{\text{ci}}(c) \neq 0$  or  $\#_{\text{ci}}(d) \neq 0$ .*

**Lemma 32.** *If the signature  $\Sigma$  is non trivial, for every  $\mathcal{C}$ -normal interpretation  $\mathcal{I}$  and every  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ ,  $\mathbf{s}^{\mathcal{I}}$  is infinite.*

*Proof.* Consider any sort  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$ . We construct a sequence of constructor terms  $t_i$  (for  $i \in \mathbb{N}$ ) of sort  $\mathbf{s}$ , by induction on the set of positions as follows. Let  $p$  be a position and assume that  $t_i(q)$  has been constructed for all positions  $q \prec p$ , where  $p$  is a position in  $\text{dom}(t_i)$  such that  $t_i(p)$  is undefined. Then  $t_i|_p$  must be of some sort  $\mathbf{t}$  (if  $p = \varepsilon$  then  $\mathbf{s} = \mathbf{t}$ , otherwise the sort  $\mathbf{t}$  is fixed by the symbol occurring at the predecessor of  $p$ : if this symbol has profile  $\mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}'$  and  $p$  is of the form  $q.j$  with  $j = 1, \dots, n$ , then  $\mathbf{t} = \mathbf{s}_j$ ). If  $\mathbf{t} \notin \mathcal{S}_{\text{ci}}$ , then we let  $t_i(p) = x$ , where  $x$  is an arbitrarily chosen variable of sort  $\mathbf{t}$ . If  $\mathbf{t} \in \mathcal{S}_{\text{ci}}$  and  $i = |p|$  then we let  $t_i|_p = c(x_1, \dots, x_n)$ , where  $c$  is a (fixed for a given  $\mathbf{t}$ ) constructor of co-domain  $\mathbf{t}$  and of arity  $n$ , and  $x_1, \dots, x_n$  are arbitrarily chosen variables of the appropriate sorts. Finally, if  $\mathbf{t} \in \mathcal{S}_{\text{ci}}$  and  $i \neq |p|$  then we let  $t_i(p) = d$ , where



$d$  is a constructor of co-domain  $\mathfrak{t}$ , distinct from  $c$ , and such that  $\#_{\text{co}}(d) > 0$ . Note that such a pair of constructors  $(c, d)$  exists for all sorts  $\mathfrak{t}$  since  $\Sigma$  is non trivial. Then all the positions  $p.i$  with  $i = 1, \dots, \#(d)$  are added in  $\text{dom}(t_i)$ . By construction,  $t_i$  necessarily contains a position  $p_i$  of length  $i$ , moreover, for all  $i, j$  with  $i < j$ , we have  $t_i(q) = t_j(q)$  for all  $q \prec p_i$ , and  $t_i(p_i) \neq t_j(p_i)$ . Thus  $[t_i]^{\mathcal{I}} \neq [t_j]^{\mathcal{I}}$ , since the constructors are injective and have disjoint ranges. Hence  $\mathfrak{s}^{\mathcal{I}}$  must be infinite.  $\square$

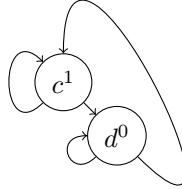
This entails that for every formula  $\phi$ , if  $\{\phi\} \cup \mathcal{A}^*$  is unsatisfiable then  $\phi$  admits no regularly co-inductive interpretation (if the signature is non trivial), thus  $\{\phi\} \cup \mathcal{A}$  is also unsatisfiable (by Theorem 30). Conversely, we show that the axioms considered in the present work are strictly stronger than  $\mathcal{A}^*$ :

**Theorem 33.** *There exists a formula  $\phi$  such that  $\{\phi\} \cup \mathcal{A}^*$  is satisfiable, but  $\phi$  admits no regularly co-inductive model.*

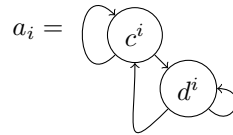
*Proof.* Consider the formula

$$\phi = a_1 \approx c(a_1, b_1) \wedge b_1 \approx d(a_1, b_1) \wedge a_2 \approx c(a_2, b_2) \wedge b_2 \approx d(a_2, b_2) \wedge a_1 \not\approx a_2$$

where  $c : \mathfrak{s}, \mathfrak{s} \rightarrow \mathfrak{s}$  and  $d : \mathfrak{s}, \mathfrak{s} \rightarrow \mathfrak{s}$  are constructors and  $a_1, a_2, b_1, b_2 \notin \mathcal{C}$ . It is clear that  $\phi$  admits no regularly co-inductive model (otherwise the infinite term  $t = c(t, s)$  with  $s = d(t, s)$  would admit two distinct regular labeling functions). Let  $\mathcal{I}$  be the interpretation defined as follows. The domain  $\mathfrak{s}^{\mathcal{I}}$  is a subset (defined inductively below) of the set of ground infinite terms  $\mathfrak{t}$  built on the signature  $f^i$ , with  $f \in \{c, d\}$  and  $i \in \mathbb{N}$  (i.e., constructors decorated by exponents). Note that all such ground terms are infinite terms, since there is no constant symbol. We denote by  $\rho(\mathfrak{t})$  the number  $i$  such that  $\mathfrak{t}(\varepsilon)$  is of the form  $f^i$  with  $f \in \{c, d\}$ . For instance if  $\mathfrak{t}$  denotes the tree:



then  $\rho(\mathfrak{t}) = 1$  and  $\rho(\mathfrak{t}|_2) = 0$ . The exponents on the constructors will be useful to ensure that the constants  $a_1$  and  $a_2$  can be interpreted as different elements, more precisely each constant  $a_i$  will be interpreted as a term with exponent  $i$ :



Before defining the domain  $[\mathbf{s}]^{\mathcal{I}}$  of  $\mathbf{s}$ , we actually define the interpretation of the function symbols  $[c]^{\mathcal{I}}$  and  $[d]^{\mathcal{I}}$ . For technical convenience, these functions will be defined on any ground term built on the signature defined above (even if it is not in  $\mathbf{s}^{\mathcal{I}}$ ). The interpretations of  $c$  and  $d$  can be considered as the restrictions of  $[c]^{\mathcal{I}}$  and  $[d]^{\mathcal{I}}$  to the set  $[\mathbf{s}]^{\mathcal{I}}$  which is defined afterwards:

- If  $\mathbf{t}, \mathbf{t}'$  are ground terms and  $f \in \{c, d\}$  then  $[f]^{\mathcal{I}}(\mathbf{t}, \mathbf{t}')$  is defined as follows:  
 $[f]^{\mathcal{I}}(\mathbf{t}, \mathbf{t}') \stackrel{\text{def}}{=} f^i(\mathbf{t}, \mathbf{t}')$ , where  $i = \max(\rho(\mathbf{t}), \rho(\mathbf{t}'))$  if  $\mathbf{t}$  or  $\mathbf{t}'$  contains a subterm of the form  $f^{\max(\rho(\mathbf{t}), \rho(\mathbf{t}'))}(\mathbf{t}, \mathbf{t}')$ ; and  $i = \max(\rho(\mathbf{t}), \rho(\mathbf{t}')) + 1$  otherwise.

For instance, if  $\mathbf{t} = c^0(\mathbf{t}, \mathbf{t})$  and  $\mathbf{t}' = d^0(\mathbf{t}', \mathbf{t}')$ , then we get:  $\rho(\mathbf{t}) = \rho(\mathbf{t}') = 0$  and  $[c]^{\mathcal{I}}(\mathbf{t}, \mathbf{t}') = c^1(\mathbf{t}, \mathbf{t}')$ , as neither  $\mathbf{t}$  nor  $\mathbf{t}'$  contains  $c^0(\mathbf{t}, \mathbf{t}')$ . In contrast, if  $\mathbf{t} = c^0(\mathbf{t}, \mathbf{t}')$  and  $\mathbf{t}' = d^0(\mathbf{t}, \mathbf{t}')$ , then we get:  $[c]^{\mathcal{I}}(\mathbf{t}, \mathbf{t}') = c^0(\mathbf{t}, \mathbf{t}') = \mathbf{t}$ .

The domain  $\mathbf{s}^{\mathcal{I}}$  is constructed as follows (using Item 1 as the base case):

1.  $\mathbf{s}^{\mathcal{I}}$  contains the infinite terms  $\mathbf{t}_i, \mathbf{t}'_i$  (for all  $i = 1, 2$ ) defined as follows:  
 $\mathbf{t}_i \stackrel{\text{def}}{=} c^i(\mathbf{t}_i, \mathbf{t}'_i)$  and  $\mathbf{t}'_i \stackrel{\text{def}}{=} d^i(\mathbf{t}_i, \mathbf{t}'_i)$ , and we let  $[a_i]^{\mathcal{I}} \stackrel{\text{def}}{=} \mathbf{t}_i$  and  $[b_i]^{\mathcal{I}} \stackrel{\text{def}}{=} \mathbf{t}'_i$ .  
Note that, by definition of  $[f]^{\mathcal{I}}$ , we have  $[c]^{\mathcal{I}}(\mathbf{t}_i, \mathbf{t}'_i) = c^i(\mathbf{t}_i, \mathbf{t}'_i) = \mathbf{t}_i$  and  $[d]^{\mathcal{I}}(\mathbf{t}_i, \mathbf{t}'_i) = d^i(\mathbf{t}_i, \mathbf{t}'_i) = \mathbf{t}'_i$ .
2. If  $t$  is a finite constructor term (satisfying the condition above) with  $x \in \mathcal{V}(t)$  and  $x \neq t$ ,  $\mathcal{J}$  is an associate of  $\mathcal{I}$  and  $\zeta \neq [t]^{\mathcal{J}\{x \leftarrow \zeta\}}$  holds for all  $\zeta \in \{\mathbf{t}_1, \mathbf{t}_2, \mathbf{t}'_1, \mathbf{t}'_2\}$  and for all subtrees  $\zeta$  of  $y^{\mathcal{J}}$ , with  $y \in \mathcal{V}(t) \setminus \{x\}$ , then we add in  $\mathbf{s}^{\mathcal{I}}$  the term  $\mathbf{t}$  (and all its subterms) obtained from  $t$  as follows: every occurrence of  $x$  is replaced by  $\mathbf{t}$ , every variable  $y \neq x$  is replaced by  $[y]^{\mathcal{J}}$  and every symbol  $f$  is replaced by  $f^i$ , where  $i = 0$  if  $t$  contains no variable other than  $x$  and otherwise  $i = 1 + \max(\{\rho(y^{\mathcal{J}}) \mid y \in \mathcal{V}(t), y \neq x\})$ . By construction,  $\mathbf{t} = [t]^{\mathcal{J}\{x \leftarrow \mathbf{t}\}}$ , i.e.,  $\mathbf{t}$  is a solution of the fixpoint equation  $x \approx t$ . Thus this condition ensures that every fixpoint equation admits at least one solution, by adding one such solution in the domain. The conditions ensure that the domain does not already contain such a solution.
3. If  $\mathbf{t}, \mathbf{t}' \in \mathbf{s}^{\mathcal{I}}$  then  $[f]^{\mathcal{I}}(\mathbf{t}, \mathbf{t}') \in \mathbf{s}^{\mathcal{I}}$  (for  $f \in \{c, d\}$ ). This condition ensures that  $[\mathbf{s}]^{\mathcal{I}}$  is closed under  $[c]^{\mathcal{I}}$  and  $[d]^{\mathcal{I}}$ . Note that it adds new elements in the domain only if  $\mathbf{t}, \mathbf{t}'$  do not already contain  $[f]^{\mathcal{I}}(\mathbf{t}, \mathbf{t}')$ , hence if  $[f]^{\mathcal{I}}(\mathbf{t}, \mathbf{t}')$  does not properly occur in itself.

To illustrate Item 2, assume that Item 1 has already been applied and consider the term  $t = c(x, x)$  (the associate  $\mathcal{J}$  is irrelevant here since  $t$  contains no variable other than  $x$ ). Since none of the terms  $\mathbf{t}_1, \mathbf{t}_2, \mathbf{t}'_1, \mathbf{t}'_2$  is a solution of  $x \approx c(x, x)$ , the term  $\mathbf{t} = c^0(\mathbf{t}, \mathbf{t})$  is added in  $[\mathbf{s}]^{\mathcal{I}}$ . Afterwards, one might also consider the term  $t' = c(y, x)$ , with the associate  $[y]^{\mathcal{J}} \stackrel{\text{def}}{=} \mathbf{t}$  (note that considering this associate is possible only after  $\mathbf{t}$  is added into the domain). Here the term  $\mathbf{t}' = c^1(\mathbf{t}, \mathbf{t}')$  could be added as a solution of the equation  $x \approx c(y, x)$ , but this is prevented by the condition  $\zeta \neq [t]^{\mathcal{J}\{x \leftarrow \zeta\}}$  in Item 2, as  $\mathbf{t}$  is already a solution of this equation. However, we may also consider the same term  $t'$  with the associate  $[y]^{\mathcal{J}'} \stackrel{\text{def}}{=} \mathbf{t}_1$ , which triggers the addition of the term  $\mathbf{t}'' = c^1(\mathbf{t}_1, \mathbf{t}'')$  into the domain. The key point here is that one needs to include sufficiently many trees in the domain to ensure that every fixpoint equation admits a solution, but at the same time one cannot keep all infinite trees, as otherwise some equations will have several solutions.

It is straightforward to verify that  $[c]^{\mathcal{I}}$  is injective, that  $c^{\mathcal{I}}, d^{\mathcal{I}}$  have disjoint domains, that every term in  $\mathbf{s}^{\mathcal{I}}$  is of the form  $[f]^{\mathcal{I}}(\mathbf{t}, \mathbf{t}')$  with  $f \in \{c, d\}$  and  $\mathbf{t}, \mathbf{t}' \in \mathbf{s}^{\mathcal{I}}$  and that  $\mathbf{s}^{\mathcal{I}}$  is infinite. By Item 2, every fixpoint equation admits a solution. By Item 1, we have  $\mathcal{I} \models \phi$ . It only remains to prove that the solution of every fixpoint equation is unique. Let  $t$  be a term and let  $x$  be a variable properly occurring in  $t$ . Let  $\mathcal{J}$  be an associate of  $\mathcal{I}$ . Let  $\zeta_i$  (for  $i = 1, 2$ ) be distinct solutions of the fixpoint equation  $x \approx t$ , i.e.,  $\zeta_i = [t]^{\mathcal{J}\{x \leftarrow \zeta_i\}}$  (for all  $i = 1, 2$ ) and  $\zeta_1 \neq \zeta_2$ . We distinguish several cases.

- If  $\zeta_i$  (for some  $i = 1, 2$ ) is introduced in  $\mathbf{s}^{\mathcal{I}}$  by Item 3, then it is clear that  $\zeta_i$  cannot be a proper subterm of  $\zeta_i$ , hence  $\zeta_i$  cannot be the solution of a fixpoint equation. Thus this case cannot occur.
- If both  $\zeta_1$  and  $\zeta_2$  are introduced by Item 1 then, since  $\zeta_1$  and  $\zeta_2$  have no common subterm, necessary  $t$  contains no variable other than  $x$ . But then  $t$  necessarily contains at least one subterm of the form  $f(x, x)$  (with  $f \in \{c, d\}$ ), thus  $[t]^{\mathcal{J}\{x \leftarrow \zeta_i\}}$  contains a subterm  $f^j(\zeta_i, \zeta_i)$ . This case cannot occur since  $\zeta_i = [t]^{\mathcal{J}\{x \leftarrow \zeta_i\}}$  and  $\zeta_i$  contains no such subterm.
- Assume that both  $\zeta_1$  and  $\zeta_2$  are introduced by Item 2 on some terms  $s_i$  and associates  $\mathcal{J}_i$  of  $\mathcal{I}$ . Let  $P_i$  be the set of positions in  $\zeta_i$  such that  $\zeta_i|_p$  is a proper subterm of  $\zeta_i$ . As  $\zeta_i = [t]^{\mathcal{J}\{x \leftarrow \zeta_i\}}$ , we have, for all positions  $p$  in  $t$ :
  - If  $t|_p$  does not contain  $x$  then  $\zeta_i|_p = [t|_p]^{\mathcal{J}}$ .
  - If  $t|_p = x$  then  $\zeta_i|_p = \zeta_i$ .
  - Otherwise  $\zeta_i(p)$  must be of the form  $t(p)^{k_i}$ , with  $k_i = \rho(\zeta_i)$ .

This entails that  $\zeta_1$  and  $\zeta_2$  only differ by their exponents. Moreover, by Item 2, either  $k_i = 0$  and  $P_i = \emptyset$ , or  $k_i = \max(\{\rho(\zeta_i|_p) \mid p \in P_i\}) + 1$ . Thus, if  $P_1 = P_2$ , then necessarily  $\zeta_1 = \zeta_2$ , which contradicts our assumption. Therefore  $P_1 \neq P_2$ , and we may assume, by symmetry, that there exists a position  $p \in P_1 \setminus P_2$ . Then (by the above assumption on fixpoint equations)  $t|_p$  must be a variable  $y$ , and  $\zeta_1$  occurs in  $y^{\mathcal{J}_2}$ . Thus  $\zeta_1$  is introduced before  $\zeta_2$ . As the converse cannot simultaneously hold, necessarily  $P_1 \supset P_2$ , which entails that we have  $\rho(\zeta_2|_p) = \rho(\zeta_2|_q) \Rightarrow \rho(\zeta_1|_p) = \rho(\zeta_1|_q)$ , for all positions  $p, q$ . Since  $\zeta_2 = [s_2]^{\mathcal{J}\{x \leftarrow \zeta_2\}}$ , we get  $\zeta_1 = [s_2]^{\mathcal{J}\{x \leftarrow \zeta_1\}}$ , which contradicts the condition in Item 2.

- If  $\zeta_i$  is introduced by Item 2 on some term  $s_i$ , and  $\zeta_{3-i}$  is introduced by Item 1, then, as  $\zeta_i$  and  $\zeta_{3-i}$  only differ by the value of exponents, and  $\zeta_{3-i}$  has only one exponent, we get  $\zeta_{3-i} = [s_i]^{\mathcal{J}\{x \leftarrow \zeta_{3-i}\}}$ , which is impossible, by definition of Item 2.

□

## 4 A Resolution Proof Procedure to Handle Co-Inductive Data Structures

Building on the previous results, we devise proof calculi for reasoning with co-inductive structures. We first show (see Theorems 41 and 44) that the axioms

ensuring the existence of a regular labeling function (Lemma 29) can be omitted if rational terms are directly handled by the proof procedure and unification algorithm. The notions of literals, clauses etc. are defined as usual (where atoms are defined on rational terms), see for instance [20]. The empty clause is denoted by  $\square$ .

**Definition 34.** A substitution  $\sigma$  is a function mapping every variable  $x$  to a rational term  $x\sigma$  of the same sort as  $x$ . We denote by  $\text{dom}(\sigma)$  the set of variables  $x$  such that  $x\sigma \neq x$ , and by  $\text{id}$  the substitution such that  $\text{dom}(\text{id}) = \emptyset$ . For every variable  $x$  and for every term  $t$  of the same sort as  $x$ , we denote by  $\{x \leftarrow t\}$  the substitution of domain  $\{x\}$  mapping  $x$  to  $t$ .  $t\sigma$  is the term obtained from  $t$  by replacing every occurrence of a variable  $x$  in  $t$  by  $x\sigma$ . We denote by  $\sigma\theta$  the composition of  $\sigma$  and  $\theta$  and we write  $\sigma \geq \theta$  if  $\theta = \sigma\eta$ , for some substitution  $\eta$ . A substitution  $\sigma$  is a unifier of two terms  $t$  and  $s$  if  $t\sigma = s\sigma$ . It is well-known that every unifiable pair of terms admits a most general unifier<sup>5</sup> (mgu), that is unique up to a renaming of variables, i.e., a unifier that is maximal w.r.t.  $\geq$ . For every clause  $C$  we denote by  $I_g(C)$  the set of ground instances  $C\sigma$  of  $C$ . If  $S$  is a set of clauses then  $I_g(S) \stackrel{\text{def}}{=} \bigcup_{C \in S} I_g(C)$ .

We denote by  $\mathcal{E}$  the axioms of equality, defined as follows:

$$(x \approx x) \wedge (x \approx y \Rightarrow y \approx x) \wedge (x \approx y \wedge y \approx z \Rightarrow x \approx z) \quad (15)$$

for all sorts  $\mathbf{s}$ , where  $x, y$  and  $z$  are pairwise distinct variables of sort  $\mathbf{s}$ ;

$$\left( \bigwedge_{i=1}^n x_i \approx y_i \right) \Rightarrow f(x_1, \dots, x_n) \approx f(x_1, \dots, x_n) \quad (16)$$

for all  $f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s} \in \Sigma$  (with  $\mathbf{s} \neq \text{bool}$ ) where  $x_i, y_i$  (for  $i \in \{1, \dots, n\}$ ) are pairwise distinct variables of sort  $\mathbf{s}_i$ ;

$$\left( \bigwedge_{i=1}^n x_i \approx y_i \right) \wedge P(x_1, \dots, x_n) \Rightarrow P(y_1, \dots, y_n) \quad (17)$$

for all  $P : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s} \in \text{bool}$ , where  $x_i, y_i$  (for  $i \in \{1, \dots, n\}$ ) are pairwise distinct variables of sort  $\mathbf{s}_i$ .

Let  $\succeq$  be a partial order<sup>6</sup> among atoms, that is total on ground atoms and closed under substitution, i.e.,  $\alpha \succeq \beta \implies \alpha\sigma \succeq \beta\sigma$ , for all atoms  $\alpha, \beta$  and for all substitutions  $\sigma$ . We denote by  $\succ$  the associated strict order, i.e.,  $\alpha \succ \beta \iff (\alpha \succeq \beta \wedge \alpha \neq \beta)$ . The order  $\succeq$  is extended to literals as follows. For all atoms  $\alpha, \beta$ :  $\neg\alpha \succ \alpha$  and  $\alpha \succ \beta \implies \neg\alpha \succ \neg\beta$ . Let  $\text{sel}$  be a selection function mapping every clause  $C$  to a (possibly empty) set of negative literals in  $C$ . We assume to simplify technicalities that  $\text{sel}$  is *liftable*, i.e.,  $l\sigma \in \text{sel}(C\sigma) \implies l \in \text{sel}(C)$  holds for all literals  $l$ , clauses  $C$  and substitutions  $\sigma$ . A literal  $l$  is *eligible* in a clause  $C$  if either  $l \in \text{sel}(C)$  or  $\text{sel}(C) = \emptyset$  and  $l$  is maximal in  $C$  (w.r.t.  $\succeq$ ). The first two inference rules are standard (see, e.g., [20, 3]). Eligible literals are highlighted with a grey background. We assume as usual that the premises share no variables.

<sup>5</sup>The mgu may be computed by using usual unification algorithms, where the occur check rule is restricted to non constructor positions.

<sup>6</sup>i.e., a transitive, antisymmetric and reflexive relation.

$$\text{Resolution (Res): } \frac{\alpha \vee C \quad \neg\beta \vee D}{(C \vee D)\sigma}$$

if  $\sigma = mgu(\alpha, \beta)$ ,  $\alpha\sigma$  is eligible in  $(\alpha \vee C)\sigma$  and  $\neg\beta\sigma$  is eligible in  $(\neg\beta \vee D)\sigma$ .

$$\text{Factorisation (Fact): } \frac{\alpha \vee \beta \vee C}{(\alpha \vee C)\sigma}$$

if  $\sigma = mgu(\alpha, \beta)$ ,  $\alpha\sigma$  is eligible in  $(\alpha \vee \beta \vee C)\sigma$ .

**Proposition 35.** *If  $l\sigma$  is eligible in  $(l \vee C)\sigma$  then  $l$  is eligible in  $l \vee C$ .*

*Proof.* This follows immediately from the fact that  $\succeq$  is closed under substitution and that *sel* is liftable.  $\square$

We now define a new inference rule, called *Cycle*, to identify fixpoint equations and infer their solutions. For instance, if the equation  $t \approx c(t)$  holds with  $c \in \mathcal{C}$ , then the rule will compute the infinite term  $u = c(c(\dots))$  and will derive the equation  $t \approx u$ .

**Definition 36.** *For all terms  $t$  and for all constructor positions  $p$  in  $t$ ,  $t[\circ]_p$  denotes the (unique) term such that  $t[\circ]_p = t[t[\circ]_p]_p$ , formally defined as follows:  $\text{dom}(t[\circ]_p) \stackrel{\text{def}}{=} \{p^n.r \mid n \geq 0, r \in \text{dom}(t), p \not\prec r\}$  and  $t[\circ]_p(q) \stackrel{\text{def}}{=} t(r)$  if  $q = p^n.r, n \geq 0, r \in \text{dom}(t)$  and  $p \not\prec r$ .*

**Proposition 37.** *Let  $t$  be a term and let  $\sigma$  be a substitution. If  $p \in \text{dom}(t)$  then  $t[\circ]_p\sigma = (t\sigma)[\circ]_p$ .*

*Proof.* Immediate.  $\square$

**Definition 38.** *A term  $t$  is a  $p$ -term if  $p$  is a constructor position in  $t$  and for every position  $q \in \text{dom}(t)$  such that  $q \not\prec p$ , we have  $t(q) \in \mathcal{V}$ . Note that this entails that  $t$  is finite and that all the functions occurring in  $t$  are constructors.*

For instance, if  $c, d$  are constructors and  $x, y, z$  are variables, then the term  $c(x, d(y, z))$  is a 2.2-term and a 2.1-term but not a 1-term or a 2-term. The rule *Cycle* is defined as follows:

$$\text{Cycle (Cyc): } \frac{t \approx s \vee C}{(t\theta \approx (s\theta)[\circ]_p \vee C\theta)\sigma}$$

if  $\sigma = mgu(t\theta, s\theta|_p)$ ,  $(t \approx s)\theta\sigma$  is eligible in  $(t \approx s \vee C)\theta\sigma$  and either  $p \in \text{dom}(s)$  and  $\theta = id$ ; or  $p = q.r, q \in \text{dom}(s), s|_q = x$ , and  $\theta = \{x \leftarrow u\}$  for some  $r$ -term  $u$  of the same sort as  $x$ .

Note that *Cycle* applies in two ways, either at some position  $p$  in  $s$  (first case above), or at some position  $p$  that is “below” a variable occurring at some position  $q$  in  $s$  (second case). This is meant to ensure that the rule is “liftable”, in the sense that the applications of the rule on some non ground clause  $C$  simulate all applications on ground instances of  $C$  (see Lemma 40).

**Example 39.** *Given the clause  $f(a) \approx c(x, y) \vee P(y)$  (with  $c \in \mathcal{C}$ ), *Cyc* may be applied on the position 2 in  $c(x, y)$ , with substitution *id* and unifier  $\{y \leftarrow f(a)\}$ , yielding  $f(a) \approx t \vee P(f(a))$ , where  $t$  is the infinite term  $t = c(x, t)$ . But it may be also applied (for instance) on the position 2.2 and 2-term  $c(z, w)$ , yielding:  $f(a) \approx s \vee P(c(z, f(a)))$ , with  $s = c(x, c(z, s))$ .*

Note that the rule **Cyc** is infinitely branching (since the position  $p$  is of arbitrary length). It is defined in such a way that it is “liftable”, in the following sense:

**Lemma 40.** *If a clause  $C$  is deduced from a ground instance  $D\sigma$  of some clause  $D$  by one application of the rule **Cyc**, then there exists an application of **Cyc** on  $D$  that yields a clause  $E$  such that  $C = E\theta$ , for some ground substitution  $\theta$ .*

*Proof.* Note that the application of **Cyc** on  $D\sigma$  uses the substitution  $id$  since by hypothesis  $D\sigma$  contains no variable. By definition,  $D$  is of the form  $(t \approx s) \vee D'$ ,  $(t \approx s)\sigma$  is eligible in  $(t \approx s \vee D')\sigma$ ,  $s\sigma|_p = t\sigma$ , and  $C = t\sigma \approx s\sigma[\odot]_p \vee D'\sigma$ . We distinguish two cases.

- $p \in \text{dom}(s)$ . In this case, we have  $s\sigma|_p = s|_p\sigma$ , thus  $s|_p$  and  $t$  have an mgu  $\eta$ , with  $\sigma = \eta\theta$ . Moreover, by Proposition 35,  $(t \approx s)\eta$  is eligible in  $D\eta$ . We may thus apply the rule **Cyc** on  $D$ , with the position  $p$  and the substitution  $id$ , yielding:  $E = t\eta \approx s[\odot]_p\eta \vee D'\eta$ . We have  $E\theta = t\sigma \approx s[\odot]_p\sigma \vee D'\sigma$ . By Proposition 37,  $s[\odot]_p\sigma = s\sigma[\odot]_p$ , hence  $E\theta = C$ .
- $p \notin \text{dom}(s)$ . Since  $p \in \text{dom}(s\sigma)$ , necessarily there exist positions  $q, r$  such that  $p = q.r$  and  $s|_q$  is a variable  $x$ . Let  $u$  be the term obtained from  $x\sigma$  by replacing all subterms occurring at some position  $p'$  with  $p' \neq r$  by fresh, pairwise distinct, variables. Since  $p$  is a constructor position in  $s$ ,  $u$  is an  $r$ -term. Moreover, it is clear that there exists a substitution  $\sigma'$  such that  $u\sigma' = x\sigma$ , so that  $\{x \leftarrow u\}\sigma\sigma' = \sigma\sigma'$ . By definition, the term  $s\{x \leftarrow u\}|_p$  is a variable occurring in  $u$  (hence not occurring in  $D$ ). Thus  $s\{x \leftarrow u\}|_p$  and  $t$  admit an mgu  $\eta$ . Furthermore, there exists a substitution  $\theta$  such that  $\sigma\sigma' = \eta\theta$ , since  $t\sigma\sigma' = t\sigma = s\sigma|_p = s\{x \leftarrow u\}\sigma\sigma'|_p = s\{x \leftarrow u\}|_p\sigma\sigma'$ . By Proposition 35,  $(t \approx s)\{x \leftarrow u\}\eta$  is eligible in  $D\{x \leftarrow u\}\eta$ . We may thus apply the rule **Cyc** on  $D$ , with the position  $p = q.r$ , the  $r$ -term  $u$  and the substitution  $\{x \leftarrow u\}$ , yielding:  $E = t\{x \leftarrow u\}\eta \approx s\{x \leftarrow u\}[\odot]_p\eta \vee D'\{x \leftarrow u\}\eta$ . We have  $E\theta = t\{x \leftarrow u\}\eta\theta \approx s\{x \leftarrow u\}[\odot]_p\eta\theta \vee D'\{x \leftarrow u\}\eta\theta$ . Since  $\{x \leftarrow u\}\sigma'\sigma = \sigma'\sigma$  we get (using Proposition 37):  $E\theta = t\sigma \approx s\sigma[\odot]_p \vee D'\sigma = C$ .

□

We write  $S \vdash_{\mathbf{R}} C$  if  $C$  is deducible from premises in  $S$  by some rule in the set  $\mathbf{R}$  (in a single step), and  $S \vdash_{\mathbf{R}}^* C$  if there exists a sequence  $C_1, \dots, C_n$  (with  $n \geq 1$ ) such that  $C_n = C$  and  $S \cup \{C_1, \dots, C_i\} \vdash_{\mathbf{R}} C_{i+1}$  holds for every  $i = 0, \dots, n-1$ .

**Theorem 41.** *The rules **Res**, **Fact** and **Cyc** are sound (w.r.t. regularly co-inductive interpretations), i.e., if  $S \vdash_{\{\mathbf{Res}, \mathbf{Fact}, \mathbf{Cyc}\}} C$  then every regularly co-inductive model of  $S$  is a model of  $C$ . In particular, if  $S \vdash_{\{\mathbf{Res}, \mathbf{Fact}, \mathbf{Cyc}\}}^* \square$  then  $S$  admits no regularly co-inductive model.*

*Proof.* The soundness of the rules **Res** and **Fact** is routine (see for example [20]) and the addition of rational terms has no impact on it. We only provide the proof for the rule **Cyc** (the second statement follows by an immediate induction on the length of the derivation). Let  $(t \approx s[\odot]_p \vee C)\theta\sigma$  be a clause deduced from a clause  $t \approx s \vee C \in S$  using **Cyc**. We assume that  $\theta = id$ . Indeed, if  $\theta$  is of the form  $\{x \leftarrow u\}$  for some  $r$ -term  $u$  with  $p = q.r$  and  $s|_q = x$ , then it is clear that the clause  $(t \approx s[\odot]_p \vee C)\theta\sigma$  can also be obtained by applying **Cyc**

on the premise  $t\theta \approx s\theta \vee C\theta$ , with the same position  $p$  and mgu  $\sigma$  and with the substitution  $id$  (since by definition  $p$  is a position in  $s\theta$ ). Since the considered premise is a logical consequence of  $t \approx s \vee C$ , the result follows.

Let  $\mathcal{I}$  be a regularly co-inductive model of  $S$ . Since all variables in a clause are universally quantified, we deduce that  $\mathcal{I} \models (t \approx s \vee C)\sigma$ , thus either  $\mathcal{I} \models (t \approx s)\sigma$  or  $\mathcal{I} \models C\sigma$  (we remind that interpretations also interpret variables). If  $\mathcal{I} \models C\sigma$  then  $\mathcal{I} \models (t \approx s[\odot]_p \vee C)\sigma$  and the proof is completed. If  $\mathcal{I} \models (t \approx s)\sigma$ , we have  $[t\sigma]^\mathcal{I} = [s\sigma]^\mathcal{I}$ , and by definition of  $\sigma$ ,  $s|_p\sigma = t\sigma$ .

Let  $u = s[\odot]_p\sigma$ . We define a function  $\mu$  mapping positions in  $u$  to elements of the domain of  $\mathcal{I}$  as follows. By definition of  $s[\odot]_p$ , every position  $q$  in  $u$  can be uniquely decomposed as a position of the form  $p^n.r$ , for some  $n \geq 0$  and some position  $r \in \text{dom}(s\sigma)$ , with  $p \not\leq r$ . Then we set:  $\mu(q) \stackrel{\text{def}}{=} [s\sigma|_r]^\mathcal{I}$ . We show that  $\mu$  is a regular labeling function, i.e., that it satisfies Conditions 1, 2 and 3 in Definition 11.

- 1 Assume that  $u|_q$  is a variable  $x$ . Then  $u|_q = s\sigma|_r = x$  and  $[s\sigma|_r]^\mathcal{I} = x^\mathcal{I}$ .
- 2 Assume that  $u|_q$  is function symbol  $f$  (of some arity  $m$ ). Then we have  $s\sigma|_r = f$  and for every  $i = 1, \dots, m$ ,  $r.i$  is a position in  $s\sigma$ , with  $[u|_q]^\mathcal{I} = [s\sigma|_r]^\mathcal{I} = f^\mathcal{I}([s\sigma|_{r.1}]^\mathcal{I}, \dots, [s\sigma|_{r.m}]^\mathcal{I})$ . If  $r.i \neq p$ , then  $q.i = p^n.(r.i)$  with  $p \not\leq r.i$ , thus we get  $u|_{q.i} = s\sigma|_{r.i}$ . If  $r.i = p$  then we have  $p.i = p^{n+1}.\varepsilon$ , so that  $[u|_{q.i}]^\mathcal{J} = [s\sigma]^\mathcal{I}$ . Since  $[t\sigma]^\mathcal{I} = [s\sigma]^\mathcal{I}$  we get  $[u|_{q.i}]^\mathcal{J} = [t\sigma]^\mathcal{I}$ , thus  $[u|_{q.i}]^\mathcal{J} = [s|_p\sigma]^\mathcal{I} = [s|_{r.i}\sigma]^\mathcal{I}$  as  $s|_p\sigma = t\sigma$ . Thus in both cases, we have  $[u|_{q.i}]^\mathcal{J} = [s|_{r.i}\sigma]^\mathcal{I}$ , and consequently,  $[u|_q]^\mathcal{J} = f^\mathcal{I}([u|_{r.1}]^\mathcal{I}, \dots, [u|_{r.m}]^\mathcal{I})$ .
- 3 Let  $u'$  be a term. Since  $s$  and  $\sigma$  are rational, the set of terms  $s\sigma|_r$  is finite. Thus the image of  $\mu$  is necessarily finite, and in particular the set  $\{\mu(q) \mid u|_q = u'\}$  is finite.

By unicity of the regular labeling function, we get  $\mu(\varepsilon) = [u]^\mathcal{I}$ , hence  $[u]^\mathcal{I} = [s\sigma]^\mathcal{I} = [t\sigma]^\mathcal{I}$ . Thus  $\mathcal{I} \models (t \approx s[\odot]_p \vee C)\sigma$ .  $\square$

Following [2], completeness is defined w.r.t. the usual notion of redundancy, that must, in our context, be defined w.r.t. a notion of propositional interpretation (as equality is not built-in).

**Definition 42.** A propositional interpretation is a set of ground literals  $\mathcal{I}$  such that, for every ground atom  $\alpha$ :  $\alpha \in \mathcal{I} \iff \neg\alpha \notin \mathcal{I}$ . For every ground clause  $C$ , we write  $\mathcal{I} \models C$  if  $C$  contains a literal in  $\mathcal{I}$ . For every non ground clause  $C$ , we write  $\mathcal{I} \models C$  if  $\mathcal{I} \models D$ , for all  $D \in I_g(C)$ , and for every set of clauses  $S$ ,  $\mathcal{I} \models S$  if  $\mathcal{I} \models C$  holds for all  $C \in S$ . We write  $S \models C$  if the implication  $\mathcal{I} \models S \implies \mathcal{I} \models C$  holds for all propositional interpretations  $\mathcal{I}$ .

**Definition 43.** (Saturated sets) Let  $S$  be a set of clauses. A ground clause  $C$  is redundant w.r.t.  $S$  if there exist clauses  $C_1, \dots, C_n \in I_g(S)$  such that  $C \succeq C_i$  (for all  $i = 1, \dots, n$ ) and  $\{C_1, \dots, C_n\} \models C$ . A non ground clause  $C$  is redundant w.r.t.  $S$  if all its ground instances are redundant. A set of clauses is saturated w.r.t. a set of rules  $R$  if every clause  $C$  such that  $S \vdash_R C$  is redundant in  $S$ .

**Theorem 44.** Let  $S$  be a set of clauses that is saturated w.r.t.  $\{\text{Res}, \text{Fact}\}$  and that contains the equality axioms, as well as Axioms 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 and 14 (as defined in Section 3.2). If  $\square \notin S$  then  $S$  admits a regularly co-inductive model.

Note that Rule **Cyc** and Axioms **12**, **13** are not needed.

*Proof.* The model is constructed in a standard way from saturated sets (see, e.g., [3]), except that the domain is the set of rational ground terms. This is sufficient to guarantee that every term has a regular labeling function. Lemmata **27** and **28** are used to prove that the constructed model is  $\mathcal{C}$ -normal and that labeling functions are unique, respectively.

More precisely, we define a propositional interpretation  $\mathcal{M}$  satisfying the assertion  $\mathcal{M} \models I_g(S)$  inductively as follows (this part of the proof is standard, but it is repeated here to ensure that the paper is self-contained).

- A positive literal  $\alpha$  is in  $\mathcal{M}$  iff there exists a clause  $\alpha \vee C \in I_g(S)$  such that for all literals  $l \in C$ ,  $\alpha \succ l$  and  $l \notin \mathcal{M}$ .
- A negative literal  $\neg\alpha$  is in  $\mathcal{M}$  iff  $\alpha \notin \mathcal{M}$ .

Note that the definition of  $\mathcal{M}$  is well-founded. We show that every clause  $C \in I_g(S)$  contains a literal in  $\mathcal{M}$ . Let  $C$  be the minimal clause in  $I_g(S)$  not satisfying this condition (where clauses are ordered using the multiset extension of the order  $\succeq$  on literals). Since  $\square \notin S$ ,  $C$  contains an eligible literal, hence by definition of  $I_g(S)$   $C$  is of the form  $(l \vee C')\sigma$ , where  $l \vee C' \in S$  and  $l\sigma$  is eligible in  $(l \vee C')\sigma$ . We distinguish two cases.

- If  $l$  is a negative literal  $\neg\alpha$ , then, since  $l\sigma \notin \mathcal{M}$ , necessarily  $\alpha\sigma \in \mathcal{M}$ , and by definition of  $\mathcal{M}$ , there exists a clause  $\beta \vee D \in S$  and a substitution  $\theta$  such that  $\alpha\sigma = \beta\theta$ ,  $\mathcal{M} \not\models D\theta$  and  $\beta\theta \succ D\theta$ . Then  $\alpha$  and  $\beta$  have an mgu  $\eta$  and there exists  $\gamma$  such that  $\eta\gamma = \sigma\theta$  (we assume w.l.o.g. that  $l \vee C'$  and  $\beta \vee D$  share no variable). By Proposition **35**, the literals  $l\eta$  and  $\alpha\eta$  are eligible in  $(l \vee C')\eta$  and  $(\beta \vee D)\eta$ , respectively. We deduce that the clause  $(C' \vee D)\eta$  is deducible from  $l \vee C'$  and  $\alpha \vee D$  by **Res**. Since  $S$  is saturated, in particular, there exist clauses  $C_1, \dots, C_n \in I_g(S)$  such that  $(C' \vee D)\eta\gamma \succeq C_i$  and  $\{C_1, \dots, C_n\} \models (C' \vee D)\eta\gamma$ . Since  $l\sigma \succ \beta\theta \succ D\theta$ , we have  $C \succ (C' \vee D)\eta\gamma$ , so that  $C \succ C_i$ , for all  $i = 1, \dots, n$ . By minimality of  $C$ , we get  $\mathcal{M} \models C_i$  (for all  $i = 1, \dots, n$ ), thus  $\mathcal{M} \models (C' \vee D)\eta\gamma$ . Since  $\mathcal{M} \not\models D\eta\gamma = D\theta$ , this entails that  $\mathcal{M} \models C'\eta\gamma$ , hence  $\mathcal{M} \models C$ , which contradicts our assumption.
- If  $l$  is a positive literal, then, since  $l\sigma$  is eligible in  $C$ , it must be maximal. We cannot have  $l\sigma \succ C'\sigma$  (as otherwise we would have  $l\sigma \in \mathcal{M}$  by definition of  $l$ ). Thus  $C'$  is of the form  $l' \vee C''$ , with  $l'\sigma = l\sigma$ . This entails that  $l$  and  $l'$  have an mgu  $\theta$ , with  $\sigma = \theta\eta$ . Then the rule **Fact** can be applied on  $l \vee l' \vee C''$ , yielding:  $l\theta \vee C''\theta$ . Since  $S$  is saturated, there exist clauses  $C_1, \dots, C_n \in I_g(S)$  such that  $l\theta\gamma \vee C''\theta\gamma \succeq C_i$  (for  $i = 1, \dots, n$ ) and  $\{C_1, \dots, C_n\} \models l\theta\gamma \vee C''\theta\gamma$ . Since  $C \succ l\theta\gamma \vee C''\theta\gamma$  we deduce by minimality of  $C$  that  $\mathcal{M} \models C_i$  (for all  $i = 1, \dots, n$ ), so that  $\mathcal{M} \models l\theta\gamma \vee C''\theta\gamma \equiv C$ , which contradicts our assumption.

Let  $\sim$  be the relation on ground terms defined as follows:  $t \sim s$  iff  $t \approx s \in \mathcal{M}$ . Since  $S$  contains all the equality axioms and  $\mathcal{M} \models I_g(S)$ , it is clear that  $\sim$  is a congruence. We denote by  $[t]_{\sim}$  the equivalence class of the term  $t$ . We define an interpretation  $\mathcal{I}$  as follows:



- For every  $\mathbf{s} \in \mathcal{S}$ ,  $\mathbf{s}^{\mathcal{I}}$  is the set of equivalence classes of ground rational terms of sort  $\mathbf{s}$ . We assume that none of these sets is empty. This is not restrictive since dummy function symbols can always be added into the signature if needed.
- For all  $n$ -ary function symbols  $f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$  and for all elements  $\zeta_i$  in  $\mathbf{s}_i^{\mathcal{I}}$  ( $i = 1, \dots, n$ ),  $f^{\mathcal{I}}(\zeta_1, \dots, \zeta_n)$  is defined as the equivalence class of  $f(t_1, \dots, t_n)$ , where  $t_i$  is an element of  $\zeta_i$ . Note that  $f^{\mathcal{I}}(\zeta_1, \dots, \zeta_n)$  does not depend on the choice of the  $t_i \in \zeta_i$ , since  $\sim$  is a congruence.
- For all  $n$ -ary predicate symbol  $P : \mathbf{s}_1, \dots, \mathbf{s}_n$  and for all elements  $\zeta_i$  in  $\mathbf{s}_i^{\mathcal{I}}$  ( $i = 1, \dots, n$ ),  $P^{\mathcal{I}}(\zeta_1, \dots, \zeta_n)$  is true iff  $P(t_1, \dots, t_n) \in \mathcal{M}$ , for some  $t_i \in \zeta_i$ .

The interpretation of variables is irrelevant since all variables are quantified universally. Note that for every associate  $\mathcal{J}$  of  $\mathcal{I}$ , and for every variable  $x$ , there exists a ground term  $t$  of the same sort as  $x$  such that  $x^{\mathcal{J}}$  is the equivalence class of  $t$ . We denote by  $\sigma_{\mathcal{J}}$  the substitution mapping every variable  $x$  to such a term  $t$  (chosen arbitrarily). For every (possibly non ground) term  $t$ , we define:  $[t]^{\mathcal{J}} \stackrel{\text{def}}{=} [t\sigma_{\mathcal{J}}]_{\sim}$ . By definition of the interpretation of predicate symbols in  $\mathcal{I}$ , this entails that, for every ground finite literal  $l$ ,  $[l]^{\mathcal{J}} = \top \iff l\sigma_{\mathcal{J}} \in \mathcal{M}$  ( $\dagger$ ). We have to prove that the mapping  $t \mapsto [t]^{\mathcal{J}}$  can indeed be associated with a regular labeling function, defined as follows: for every term  $t$ , and for every position  $p$ ,  $\mu(p) \stackrel{\text{def}}{=} [t|_p\sigma_{\mathcal{J}}]_{\sim}$  (thus in particular,  $\mu(\varepsilon) = [t]^{\mathcal{J}}$  as requested by Definition 15). We check that  $\mu$  fulfills Conditions 1, 2 and 3 in Definition 11.

- 1 Assume that  $t|_p = x \in \mathcal{V}$ . By definition  $\mu(p) = [t|_p\sigma_{\mathcal{J}}]_{\sim} = [x\sigma_{\mathcal{J}}]_{\sim} = [x]^{\mathcal{J}}$  (by definition of  $\sigma_{\mathcal{J}}$ ).
- 2 Assume that  $t|_p = f \in \Sigma$ . Then  $\mu(p) = [t|_p\sigma_{\mathcal{J}}]_{\sim}$ . Let  $n$  be the arity of  $f$ . By definition we must have, for all  $i = 1, \dots, n$ :  $p.i \in \text{dom}(t)$  and  $\mu(p.i) = [t|_{p.i}\sigma_{\mathcal{J}}]_{\sim}$ . By definition of  $\mathcal{I}$ ,  $f^{\mathcal{I}}([t|_{p.1}\sigma_{\mathcal{J}}]_{\sim}, \dots, [t|_{p.n}\sigma_{\mathcal{J}}]_{\sim}) = [f(t|_{p.1}\sigma_{\mathcal{J}}, \dots, t|_{p.n}\sigma_{\mathcal{J}})]_{\sim} = [t|_p\sigma_{\mathcal{J}}]_{\sim}$ . Thus  $\mu(p) = f^{\mathcal{I}}(\mu(p.1), \dots, \mu(p.n))$ .
- 3 By definition, for every subterm  $s$  of  $t$  the set  $\{\mu(p) \mid t|_p = s\} = \{[s\sigma_{\mathcal{J}}]_{\sim}\}$  is of cardinality 1.

We show that  $\mathcal{I} \models S$ . Consider any clause  $C \in S$  such that  $\mathcal{I} \not\models C$ . By definition,  $\mathcal{I}$  admits an associate  $\mathcal{J}$  such that  $[C]^{\mathcal{J}} = \perp$ . Since  $C\sigma_{\mathcal{J}}$  is ground,  $C\sigma_{\mathcal{J}} \in I_g(S)$ , thus  $\mathcal{M} \models C\sigma_{\mathcal{J}}$ . Therefore,  $C$  is of the form  $l \vee D$ , with  $l\sigma_{\mathcal{J}} \in \mathcal{M}$ . By  $\dagger$ , we get  $[l]^{\mathcal{J}} = \top$ , contradicting the previous assertion.

This entails that  $\mathcal{I}$  satisfies Axioms 1, 2 and 3, hence by Lemma 27,  $\mathcal{I}$  is  $\mathcal{C}$ -normal. Moreover,  $\mathcal{I}$  also satisfies Axioms 4, 5, 6, 7, 8, 9, 10, 11 and 14, hence by Lemma 28 every term admits at most one regular labeling function. Consequently,  $\mathcal{I}$  is a regularly co-inductive model of  $S$ .  $\square$

In the particular case where  $\#_{\alpha}(c) \leq 1$  for all constructors  $c \in \mathcal{C}$ , the axioms ensuring the unicity of the regular labeling function can also be omitted, if the rule  $\text{Cyc}$  is used:

**Theorem 45.** *Assume that  $\#_{\alpha}(c) \leq 1$ , for all constructors  $c \in \mathcal{C}$ . Let  $S$  be a set of clauses that is saturated w.r.t.  $\{\text{Res}, \text{Fact}, \text{Cyc}\}$  and that contains the equality axioms as well as Axioms 1, 2, 3. If  $\square \notin S$  then  $S$  admits a regularly co-inductive model.*

*Proof.* The proof is similar to that of Theorem 44, hence we focus on the parts from which it departs. The interpretation  $\mathcal{I}$  is constructed in the same way, and we prove as it is done previously that  $\mathcal{I}$  is  $\mathcal{C}$ -normal (using Axioms 1, 2, 3) and that every term admits a regular labeling function. We only have to check that for every term  $t$  and for every associate  $\mathcal{J}$  of  $\mathcal{I}$ ,  $t$  admits only one regular labeling function w.r.t.  $\mathcal{J}$ . We show that  $\mu(\varepsilon) = [t]^\mathcal{J}$  holds for every regular labeling function  $\mu$  for  $t$  w.r.t.  $\mathcal{J}$ . Since (by Proposition 13) the result holds for all subterms of  $t$ , this proves that  $\mu(p) = [t|_p]^\mathcal{J}$  holds for all  $p \in \text{dom}(t)$ , which entails that the regular labeling function is unique. We establish the result by induction on  $\text{size}(t)$ . We distinguish two cases.

- Assume first that  $t$  is not a proper subterm of  $t$ . If  $t$  is a variable, then necessarily  $\mu(\varepsilon) = x^\mathcal{J}$ , by Condition 1 in Definition 11, thus  $\mu(\varepsilon) = [t]^\mathcal{J}$ . Otherwise,  $t = f(t_1, \dots, t_n)$  with  $f \in \Sigma$  and  $\text{size}(t_i) < \text{size}(t)$  for  $i = 1, \dots, n$  (since  $t$  is not a subterm of  $t_i$ ). Let  $\mu_i$  (for  $i = 1, \dots, n$ ) be the function defined as follows:  $\mu_i(p) \stackrel{\text{def}}{=} \mu(i.p)$ . By Proposition 13,  $\mu_i$  is a regular labeling function for  $t_i$ , and by the induction hypothesis, we get  $\mu_i(\varepsilon) = [t_i]^\mathcal{J}$ . By Condition 2 in Definition 11 we have  $\mu(\varepsilon) = f^\mathcal{J}(\mu(1), \dots, \mu(n)) = f^\mathcal{J}(\mu_1(\varepsilon), \dots, \mu_n(\varepsilon)) = f^\mathcal{J}([t_1]^\mathcal{J}, \dots, [t_n]^\mathcal{J}) = [f(t_1, \dots, t_n)]^\mathcal{J} = [t]^\mathcal{J}$ .
- Now, assume that  $t$  is a proper subterm of  $t$ , i.e., there exists a position  $p$  such that  $t|_p = t$ . Then the infinite sequence  $p.p.\dots$ , is a branch in  $t$  and every symbol  $t(q)$  with  $q \preceq p$  occurs infinitely often along this branch. Since  $t$  is admissible, this entails that  $t(q) \in \mathcal{C}$ , for all  $q \preceq p$ . Since  $\#_{c_i}(c) \leq 1$ , for all constructors  $c \in \mathcal{C}$ , we must have  $p = 1^k$ , for some  $k > 0$  and for every  $i \geq 0$  and  $j > 1$  such that  $1^i.j \in \text{dom}(t)$ , the sort of  $t|_{1^i.j}$  is not in  $\mathcal{S}_{c_i}$ . This entails that  $t$  is not a subterm of  $t|_{1^i.j}$  (otherwise  $t$  would not be admissible, since the non constructor symbol  $t(1^i.j)$  would occur infinitely many often along some branch). Thus  $\text{size}(t|_{1^i.j}) < \text{size}(t)$ , and by the induction hypothesis we get  $\mu(1^i.j) = [t|_{1^i.j}]^\mathcal{J}$ .

By Condition 3 in Definition 11, and using the pigeonhole argument, necessarily there exist two constructor positions  $p_1, p_2$  in  $\{1^i \mid i \geq 0\}$  such that:  $p_2 = p_1.p'$  with  $p' \neq \varepsilon$ ,  $t|_{p_1} = t|_{p_2}$ , and  $\mu(p_1) = \mu(p_2)$ . Let  $s$  be any ground term in the equivalence class  $\mu(p_2)$  (w.r.t. the relation  $\sim$  defined in the proof of Theorem 44), and let  $u = t|_{p_2}$ . By definition,  $[u|_{p_2}]^\mathcal{J} = \mu(p_2)$ , and by Condition 2 in Definition 11, we have, for every  $q \prec p_2$ ,  $\mu(q) = f(\mu(q.1), \dots, \mu(q.m))$ , with  $f = t(q) = u(q)$  and  $m = \#(f)$ . By an easy induction on  $q$ , this entails that for every  $q \preceq p_2$ :  $[u|_q]^\mathcal{J} = \mu(q)$ . In particular,  $[u|_{p_1}]^\mathcal{J} = \mu(p_1) = \mu(p_2)$ , thus  $[u|_{p_1}]^\mathcal{J} = [s]^\mathcal{J}$ . Let  $v = u|_{p_1}$ . Note that  $v|_{p'} = u|_{p_1.p'} = u|_{p_2} = s$ . We have  $[v]^\mathcal{J} = [s]^\mathcal{J}$ , so that  $[v\sigma_\mathcal{J}]^\mathcal{I} = [s]^\mathcal{I}$ , where  $\sigma_\mathcal{J}$  denotes the substitution mapping every variable  $x$  to any ground term inside  $x^\mathcal{I}$  (note that  $s$  is ground hence its interpretation does not depend on the interpretation of the variables, hence  $[s]^\mathcal{I} = [s]^\mathcal{J}$ ).

By definition of  $\mathcal{I}$ , since  $[v\sigma_\mathcal{J}]^\mathcal{I} = [s]^\mathcal{I}$ , we have  $v\sigma_\mathcal{J} \sim s$  and  $(v\sigma_\mathcal{J} \approx s) \in \mathcal{M}$  (where  $\sim$  and  $\mathcal{M}$  are defined as in the proof of Theorem 44), hence  $I_g(S)$  contains a clause of the form  $v\sigma_\mathcal{J} \approx s \vee C$ , where  $\mathcal{M} \Vdash C$  and  $v\sigma_\mathcal{J} \approx s \succ C$ . Since  $v|_{p'} = s$ , the rule **Cyc** is applicable on this clause (with the position  $p'$  and substitution  $id$ ), yielding:  $s \approx v\sigma_\mathcal{J}[\circlearrowleft]_{p'} \vee C$ . Since  $S$  is saturated w.r.t. **Cyc**, by Lemma 40,  $I_g(S)$  is also saturated

w.r.t. **Cyc**, and the latter clause must be redundant w.r.t.  $I_g(S)$ . This implies that  $I_g(S) \models s \approx v\sigma_{\mathcal{J}}[\odot]_{p'} \vee C$ . It is easy to check that  $\models \subseteq \models$ , thus we get  $I_g(S) \models s \approx v\sigma_{\mathcal{J}}[\odot]_{p'} \vee C$ , and (since  $\mathcal{I} \models S$ ),  $\mathcal{I} \models s \approx v\sigma_{\mathcal{J}}[\odot]_{p'} \vee C$ , so that  $\mathcal{I} \models s \approx v\sigma_{\mathcal{J}}[\odot]_{p'}$  (since  $\mathcal{M} \not\models C$  and by definition  $\mathcal{I} \models l \iff \mathcal{M} \models l$  holds for all literals  $l$ , so that  $\mathcal{I} \not\models C$ ). Since  $p' \in \text{dom}(v)$ , we have (by Proposition 37)  $v\sigma_{\mathcal{J}}[\odot]_{p'} = v[\odot]_{p'}\sigma_{\mathcal{J}}$ . Thus  $[s]^{\mathcal{J}} = [s]^{\mathcal{I}} = [v[\odot]_{p'}\sigma_{\mathcal{J}}]^{\mathcal{I}} = [v[\odot]_{p'}]^{\mathcal{J}}$ . By an easy induction on the position  $p_2$ , we deduce that  $[u]^{\mathcal{J}} = [t[v[\odot]_{p'}]_{p_2}]^{\mathcal{J}}$ . Moreover, it is clear that  $v[\odot]_{p'} = t|_{p_1} = t|_{p_2}$ , so that  $t[v[\odot]_{p'}]_{p_2} = t$ . We get  $\mu(\varepsilon) = [u]^{\mathcal{J}} = [t]^{\mathcal{J}}$ .  $\square$

## 5 Handling Non-regular Labeling Functions

We now discuss the importance of Condition 3 in Definition 11 and we show that it can be discarded in some cases. The previous results depend crucially on the fact that only regular labeling functions are considered in Definition 15. More precisely, if all (rational) terms admit a unique labeling function w.r.t.  $\mathcal{I}$  then necessarily these labeling functions are regular (see Proposition 16), but Definition 15 does not prevent a term from admitting non regular labeling functions. For instance, if  $\text{prec} : \text{int} \rightarrow \text{int} \in \mathcal{C}$ , with  $\text{int}^{\mathcal{I}} = \mathbb{Z} \cup \{\infty\}$ ,  $\text{prec}^{\mathcal{I}}(x) = x - 1$  for all  $x \in \mathbb{Z}$  and  $\text{prec}^{\mathcal{I}}(\infty) = \infty$ , then the term  $t = \text{prec}(t) = \text{prec}(\text{prec}(\dots))$  admits a unique regular labeling function  $\mu$  defined as follows:  $\mu(p) \stackrel{\text{def}}{=} \infty$  for all  $p \in \text{dom}(t)$ , but it also admits infinitely many non regular labeling functions  $\mu_i$  (with  $i \in \mathbb{Z}$ ):  $\mu_i(p) \stackrel{\text{def}}{=} i + |p|$ , for all  $p \in \text{dom}(t)$ . If non regular labeling functions were considered in Definition 15 then none of the above completeness results would hold. In fact, Proposition 46 shows that no sound and complete axiomatization of the co-inductive structures possibly exists:

**Proposition 46.** *The problem of testing whether a given formula is satisfiable in some co-inductive interpretation is not co-semi-decidable.*

*Proof.* The proof is by reduction from the halting problem (for Turing machines). We encode the configurations of a Turing machine as triples

$$(x, \text{tape}(y_i, \dots, \text{tape}(y_1, \text{end}) \dots), \text{tape}(y_{i+1}, \dots, \text{tape}(y_n, \text{end}) \dots))$$

where  $\text{end}$  is a constant,  $\text{tape}$  is a binary standard function,  $x$  denotes the state,  $y_1, \dots, y_n$  denotes the content of the tape and  $i$  denotes the position of the head inside the tape. Let  $\text{next}$  be a constructor and let  $\text{run}$  be a non constructor. Every transition of the Turing machine can be associated with an equation of the form  $\text{run}(x) \approx \text{next}(\text{run}(x'))$ , where  $x$  and  $x'$  encode the initial and final configurations of the transition, respectively. A transition  $(q, a) \rightarrow (q', b, \mathbf{r})$  (where  $\mathbf{r}$  denotes a move to the right in the tape,  $q$  and  $q'$  are the initial and final states, respectively, and  $a, b$  are the symbols read and written on the tape, respectively), corresponds to the equation:  $\text{run}(q, x, \text{tape}(a, y)) \approx \text{next}(\text{run}(q', \text{tape}(b, x), y))$  whereas a transition  $(q, a) \rightarrow (q', b, \mathbf{l})$  yields the equation:  $\text{run}(q, \text{tape}(z, x), \text{tape}(a, y)) \approx \text{next}(\text{run}(q', x, \text{tape}(z, \text{tape}(b, y))))$ . The equation  $\text{end} \approx \text{tape}(B, \text{end})$  is also added, where  $B$  is the blank symbol, to enable tape extensions. Final states  $q$  are associated with the equation:

$run(q, x, y) \approx stop$ , where  $stop$  is a constructor constant. The considered machine terminates on some configuration encoded by  $u$  iff the above equations have a model  $\mathcal{I}$  (satisfying the conditions of the proposition) in which  $u \not\approx t$  holds, with  $t = next(t) = next(next(\dots))$ . Indeed, if the machine terminates then the model may be constructed as follows: the domain is  $\mathbb{N} \cup \{\infty\}$ ,  $next^{\mathcal{I}}(i) = i + 1$  if  $i \in \mathbb{N}$ ,  $next^{\mathcal{I}}(\infty) = \infty$ ,  $stop^{\mathcal{I}} = 0$ , and every term  $run(v)$  is interpreted as the length of the run from  $v$  (or  $\infty$  if the machine does not terminate). It is straightforward to check that all the above equations are satisfied and that the model satisfies the conditions of the proposition (the only infinite term  $t$  is mapped to  $\infty$ , which is the only solution of the equation  $next^{\mathcal{I}}(\infty) = \infty$ ). Conversely, if the machine does not terminate then one gets an infinite sequence of (encodings of) configurations  $s_i$  such that  $s_0 = u$  and  $s_i \approx next(s_{i+1})$  holds, for all  $i \geq 0$ . Then the function mapping every position  $1^i$  in  $dom(t)$  to the interpretation of the term  $s_i$  is a labeling function for  $t$ , and by unicity of the labeling function, this entails that  $s_0 \approx t$  holds, i.e.,  $u \not\approx t$  cannot hold. Note that the proof does not work for regularly co-inductive interpretations, since the considered labeling function is not necessarily regular. The proof follows from the fact that the halting problem is not decidable.  $\square$

We show that this theoretical limitation can be overcome in some cases, by identifying a class of clause sets for which the restriction to regular functions is not necessary. More precisely we prove that every set belonging to this class and admitting a regularly co-inductive model also admits a model in which every (arbitrary) term in fact admits exactly one regular labeling function and, moreover, in which every labeling function is actually regular. This strengthens the completeness results in Sections 3.4 and 4 by showing that they apply to a more focused class of structures. The class is defined by the following condition:

**Definition 47.** *The set of finite sorts is the least subset of  $\mathcal{S}$  satisfying the following property: if for all function symbols  $f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$ , and for all  $i = 1, \dots, n$ ,  $\mathbf{s}_i$  is finite, then  $\mathbf{s}$  is finite. A signature is  $\mathcal{S}_{\text{ci}}$ -finite, if for all function symbols  $f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$  such that  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$  and  $f \notin \mathcal{C}$ , all the sorts  $\mathbf{s}_1, \dots, \mathbf{s}_n$  are finite.*

In particular, a sort  $\mathbf{s}$  is finite if all the function symbols of range  $\mathbf{s}$  are constants (taking  $n = 0$  in Definition 47). The signature is  $\mathcal{S}_{\text{ci}}$ -finite if the considered clause set is the clausal form of a formula  $\exists x_1 \dots \exists x_n \phi$ , where the existential quantifiers inside  $\phi$  bind only variables of sorts in  $\mathcal{S}_{\text{st}}$  and the only function symbols with a co-domain in  $\mathcal{S}_{\text{ci}}$  occurring in  $\phi$  are constructors and constant symbols (after Skolemization the variables  $x_i$  will be replaced by new constant symbols, possibly of some sort in  $\mathcal{S}_{\text{ci}}$ , note that we assume, w.l.o.g., that all the non-constructor symbols in the signature occur in  $\phi$ , so that the condition of Definition 47 is trivially satisfied). We need the following:

**Proposition 48.** *If  $\mathbf{s}$  is finite, then the set  $\mathcal{T}_{\mathbf{s}}^g$  is finite. If the signature is  $\mathcal{S}_{\text{ci}}$ -finite, then the set of ground terms  $t$  such that  $t \in \mathcal{T}_{\mathbf{s}}^g$  for some  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$  and  $t(\varepsilon) \notin \mathcal{C}$  is finite.*

*Proof.* The first statement is proven by an easy induction on the set of finite sorts. The second statement follows immediately.  $\square$

**Theorem 49.** *Assume that the signature is  $\mathcal{S}_{\text{ci}}$ -finite. If a clause set  $S$  admits a regularly co-inductive model, then it admits a co-inductive model.*

*Proof.* Let  $\mathcal{I}$  be a regularly co-inductive model of  $S$ . We consider the restriction  $\mathcal{J}$  of  $\mathcal{I}$  to ground terms, formally defined as follows.

- For every  $\mathbf{s} \in \mathcal{S}$ ,  $\mathbf{s}^{\mathcal{J}} \stackrel{\text{def}}{=} \{[t]^{\mathcal{I}} \mid t \in \mathcal{T}_{\mathbf{s}}^g\}$ . We assume that for every sort  $\mathbf{s}$ ,  $\mathcal{T}_{\mathbf{s}}^g$  is not empty, so that  $\mathbf{s}^{\mathcal{J}} \neq \emptyset$  (this property can be enforced if needed by adding fresh constant symbols of profile  $\rightarrow \mathbf{s}$  for all sorts  $\mathbf{s}$ ).
- For every function symbol  $f : \mathbf{s}_1, \dots, \mathbf{s}_n \rightarrow \mathbf{s}$ , and for all  $\zeta_i \in \mathbf{s}_i^{\mathcal{J}}$ ,  $f^{\mathcal{J}}(\zeta_1, \dots, \zeta_n) \stackrel{\text{def}}{=} f^{\mathcal{I}}(\zeta_1, \dots, \zeta_n)$ . Note that  $f^{\mathcal{I}}(\zeta_1, \dots, \zeta_n) \in \mathbf{s}^{\mathcal{J}}$ , since by definition every element  $\zeta_i$  is of the form  $[t_i]^{\mathcal{I}}$ , with  $t_i \in \mathcal{T}_{\mathbf{s}_i}^g$ , so that  $f^{\mathcal{I}}(\zeta_1, \dots, \zeta_n) = f^{\mathcal{I}}([t_1]^{\mathcal{I}}, \dots, [t_n]^{\mathcal{I}}) = [f(t_1, \dots, t_n)]^{\mathcal{I}}$ , with  $f(t_1, \dots, t_n) \in \mathcal{T}_{\mathbf{s}}^g$ .
- The interpretation of variables is fixed arbitrarily. By definition, every variable  $x$  of sort  $\mathbf{s}$  is mapped to an element  $[t_x]^{\mathcal{J}}$ , with  $t_x \in \mathcal{T}_{\mathbf{s}}^g$ , and we denote by  $\sigma_{\mathcal{J}}$  the substitution mapping every variable  $x$  to  $t_x$ .

Since  $\mathcal{J}$  is a restriction of  $\mathcal{I}$ , necessarily every universal formula that is satisfied by  $\mathcal{I}$  is also satisfied by  $\mathcal{J}$ . Hence  $\mathcal{J}$  satisfies Axiom 1,2 and 3, i.e.,  $\mathcal{J}$  is  $\mathcal{C}$ -normal. Moreover, for every term  $t$ , there exists at most one regular labeling function for  $t$  w.r.t.  $\mathcal{J}$  (it is clear that the unicity of the regular labeling function can be stated as an infinite set of universal formulas). Finally, it is easy to check, as it is done in the proof of Theorem 44, that every term  $t$  admits a regular labeling function, defined as follows:  $\mu(p) \stackrel{\text{def}}{=} [t|_p \sigma_{\mathcal{J}}]^{\mathcal{J}}$ . Since the interpretation of variables are arbitrarily, the previous properties hold for all associates of  $\mathcal{J}$ , hence  $\mathcal{J}$  is regularly co-inductive.

Let  $t$  be a term, and let  $\mu$  be a labeling function for  $t$  w.r.t.  $\mathcal{I}$ . We show that  $\mu$  is regular. Assume for the sake of contradiction that the set  $\{\mu(p) \mid p \in \text{dom}(t)\}$  is infinite. This entails that there exists a branch  $p$  in  $t$  such that the set  $\{\mu(q) \mid q \preceq p\}$  is infinite. Necessarily  $p$  must be infinite, and since  $t$  is admissible, there exists a position  $q \prec p$  such that  $t(r) \in \mathcal{C}$ , for all positions  $r$  such that  $q \preceq r \prec p$ . It is clear that the set  $\{\mu(r) \mid q \preceq r \prec p\}$  is infinite. We now consider the set of elements  $\Gamma$  containing  $\mu(q)$  and all the elements  $[s]^{\mathcal{J}}$  with  $s \in \mathcal{T}_{\mathbf{s}}^g$ ,  $\mathbf{s} \in \mathcal{S}_{\text{ci}}$  and  $s(\varepsilon) \notin \mathcal{C}$ . Note that  $\Gamma$  is finite, by Proposition 48. Let  $\delta$  be a partial function mapping every element  $\zeta$  to an arbitrarily chosen regular ground term  $u$  such that  $u(\varepsilon) \in \mathcal{C}$  and  $[u]^{\mathcal{J}} = \zeta$  (if such a term exists, otherwise  $\delta(\zeta)$  is undefined). Let  $\Delta$  be the set of elements of the form  $[u]^{\mathcal{J}}$ , where  $u$  is a subterm of some term  $\delta(\zeta)$ , with  $\zeta \in \Gamma$ . Since  $\Gamma$  is finite and all the considered terms are rational,  $\Delta$  is also finite. We prove that  $\mu(r) \in \Delta$  for every  $r$  such that  $q \preceq r \prec p$ , which contradicts the fact that  $\{\mu(r) \mid q \preceq r \prec p\}$  is infinite. Note that, by definition of  $q$ ,  $t|_r = c(t_1, \dots, t_n)$ , with  $c \in \mathcal{C}$ . By definition of a labeling function (Condition 2 in Definition 11), necessarily  $\mu(r) = c^{\mathcal{I}}(\mu(r.1), \dots, \mu(r.n))$ . By definition of  $\mathcal{J}$ , every  $\mu(r.i)$  is of the form  $[s_i]^{\mathcal{J}}$ , for some  $s_i \in \mathcal{T}_{\mathbf{s}_i}^g$ , so that  $\mu(r) = c^{\mathcal{I}}([s_1]^{\mathcal{J}}, \dots, [s_n]^{\mathcal{J}}) = [c(s_1, \dots, s_n)]^{\mathcal{J}}$ . Thus  $\delta(\mu(r))$  must be defined, for all positions  $r$  such that  $q \preceq r \prec p$ . The proof is by induction on the position  $r$ . We distinguish two cases.

- Assume that  $r = q$ . Then by definition of  $\Gamma$ ,  $\mu(r) = \mu(q) \in \Gamma$ . Since  $\delta(\mu(r))$  is defined, we deduce that  $[\delta(\mu(r))]^{\mathcal{J}} \in \Delta$ , with  $\mu(r) = [\delta(\mu(r))]^{\mathcal{J}}$ . Thus  $\mu(r) \in \Delta$ .

- Assume that the property holds for some position  $r \prec p$ . Then there exists a subterm  $s$  of some ground rational term  $\delta(\zeta)$  such that  $\zeta \in \Gamma$  and  $\mu(r) = [s]^{\mathcal{J}}$ . We show that the property also holds for every position  $r.i \prec p$  (with  $i \in \mathbb{N}$ ). We distinguish two cases (let  $c = t(r)$ ).
  - $s = d(s_1, \dots, s_m)$ , where  $d \in \mathcal{C}$ . Since  $\mu(r) = c^{\mathcal{I}}(\mu(r.1), \dots, \mu(r.n))$  and  $\mathcal{J}$  is  $\mathcal{C}$ -normal, necessarily  $c = d$  and  $n = m$  (since the constructors have pairwise disjoint ranges), and  $[s_i]^{\mathcal{J}} = \mu(r.i)$  (since the constructors are injective). As  $s_i$  is a subterm of  $\delta(\zeta)$ , the proof is completed.
  - Otherwise, we have  $s \in \mathcal{T}_{\mathfrak{s}}^g$  for  $\mathfrak{s} \in \mathcal{S}_{\text{ci}}$  and  $s(\varepsilon) \notin \mathcal{C}$ , so that  $[s]^{\mathcal{J}} \in \Gamma$ . Since  $\delta(\mu(r))$  is defined,  $\delta([s]^{\mathcal{J}})$  is defined. Since  $\mu(r) = c^{\mathcal{I}}(\mu(r.1), \dots, \mu(r.n))$  and the constructors have disjoint ranges, the term  $\delta([s]^{\mathcal{J}})$  must be of the form  $c(u_1, \dots, u_n)$ , and since  $c^{\mathcal{J}}$  is injective we must have  $[u_i]^{\mathcal{J}} = \mu(r.i)$ . By definition  $u_i$  is a subterm of  $\delta([s]^{\mathcal{J}})$ , hence the proof is completed.

□

## 6 Conclusion

New axioms and proof procedures have been devised to reason on co-inductive data structures, and soundness and completeness results have been established. These completeness results have been proven to be strictly stronger than those in [6]. The axioms allow one to reduce the co-inductive satisfiability problem to a standard first-order satisfiability test. The advantage is that any first-order theorem prover can be used for this purpose, with no specific tuning. The proof procedures allow one to get rid of some of the axioms, but on the other hand the integration of the inference rules into existing provers is not straightforward. We emphasize that the proposed techniques are not restricted to regularly co-inductive structures: soundness is ensured for all co-inductive structures. Regularly co-inductive interpretations are considered mainly to provide a precise characterization of the class of structures for which the method is refutationally complete (by Proposition 46, it cannot be complete for all co-inductive structures).

We wish to mention two interesting lines of future work. First, the calculus defined in Section 4 has the drawback that it offers no built-in support for equational reasoning (the equality axioms must be added in the considered clause set). This is of course not ideal and one can hope that superposition proof procedures [2] could be defined instead of resolution calculi. This, however, is not straightforward since such proof procedures rely heavily on the existence of reduction orders, the definition of which is not clear for infinite terms (since a term can be a proper subterm of itself). Second, the rule **Cyc** has an important drawback: it is infinitely branching, meaning that infinitely many clauses may be derived from a given premise. Beside the efficiency problem, this hinders the integration of this rule into existing saturation-based provers. To overcome this, one could use variables denoting contexts, which avoids having to “guess” such contexts when the rule is applied. Such variables may be seen as second-order variables, interpreted in some particular way. While second-order unification

is undecidable in general, context unification is decidable [18]. It is not clear however whether this result extends to infinite terms.

## Acknowledgments

The author wishes to thank anonymous reviewers who provided numerous insightful comments on an earlier version of the paper.

## References

- [1] Andreas Abel, Brigitte Pientka, David Thibodeau, and Anton Setzer. Copatterns: programming infinite structures by observations. In Roberto Giacobazzi and Radhia Cousot, editors, *The 40th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '13, Rome, Italy - January 23 - 25, 2013*, pages 27–38. ACM, 2013.
- [2] L. Bachmair and H. Ganzinger. Rewrite-based equational theorem proving with selection and simplification. *Journal of Logic and Computation*, 3(4):217–247, 1994.
- [3] Leo Bachmair and Harald Ganzinger. Resolution theorem proving. In John Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning (in 2 volumes)*, pages 19–99. Elsevier and MIT Press, 2001. [doi:10.1016/b978-044450813-3/50004-7](https://doi.org/10.1016/b978-044450813-3/50004-7).
- [4] Clark Barrett, Christopher L. Conway, Morgan Deters, Liana Hadarean, Dejan Jovanović, Tim King, Andrew Reynolds, and Cesare Tinelli. CVC4. In Ganesh Gopalakrishnan and Shaz Qadeer, editors, *Proceedings of the 23<sup>rd</sup> International Conference on Computer Aided Verification (CAV '11)*, volume 6806 of *Lecture Notes in Computer Science*, pages 171–177. Springer, July 2011. Snowbird, Utah.
- [5] Julian Biendarra, Jasmin Christian Blanchette, Aymeric Bouzy, Martin Desharnais, Mathias Fleury, Johannes Hölzl, Ondrej Kuncar, Andreas Lochbihler, Fabian Meier, Lorenz Panny, Andrei Popescu, Christian Sternagel, René Thiemann, and Dmitriy Traytel. Foundational (co)datatypes and (co)recursion for higher-order logic. In Clare Dixon and Marcelo Finger, editors, *Frontiers of Combining Systems - 11th International Symposium, FroCoS 2017, Brasília, Brazil, September 27-29, 2017, Proceedings*, volume 10483 of *Lecture Notes in Computer Science*, pages 3–21. Springer, 2017.
- [6] Jasmin Christian Blanchette, Nicolas Peltier, and Simon Robillard. Superposition with datatypes and codatatypes. In Didier Galmiche, Stephan Schulz, and Roberto Sebastiani, editors, *Automated Reasoning - 9th International Joint Conference, IJCAR 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 14-17, 2018, Proceedings*, volume 10900 of *Lecture Notes in Computer Science*, pages 370–387. Springer, 2018. [doi:10.1007/978-3-319-94205-6\\_25](https://doi.org/10.1007/978-3-319-94205-6_25).
- [7] Adel Bouhoula, Emmanuel Kounalis, and Michaël Rusinowitch. Spike, an automatic theorem prover. In Andrei Voronkov, editor, *Logic Programming and Automated Reasoning, International Conference LPAR'92*,

- St. Petersburg, Russia, July 15-20, 1992, Proceedings*, volume 624 of *Lecture Notes in Computer Science*, pages 460–462. Springer, 1992. doi:  
10.1007/BFb0013087.
- [8] Robert S. Boyer and J. Strother Moore. A theorem prover for a computational logic. In Mark E. Stickel, editor, *10th International Conference on Automated Deduction, Kaiserslautern, FRG, July 24-27, 1990, Proceedings*, volume 449 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 1990. doi:10.1007/3-540-52885-7\_75.
- [9] James Brotherston. Cyclic proofs for first-order logic with inductive definitions. In B. Beckert, editor, *Automated Reasoning with Analytic Tableaux and Related Methods*, volume 3702 of *Lecture Notes in Computer Science*, pages 78–92, 2005.
- [10] Alan Bundy. The automation of proof by mathematical induction. In John Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*, pages 845–911. Elsevier and MIT Press, 2001.
- [11] Arnaud Carayol, Christof Löding, and Olivier Serre. Automata on infinite trees with equality and disequality constraints between siblings. In Martin Grohe, Eric Koskinen, and Natarajan Shankar, editors, *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '16, New York, NY, USA, July 5-8, 2016*, pages 227–236. ACM, 2016.
- [12] Liron Cohen and Reuben N. S. Rowe. Integrating induction and coinduction via closure operators and proof cycles. In Nicolas Peltier and Viorica Sofronie-Stokkermans, editors, *Automated Reasoning - 10th International Joint Conference, IJCAR 2020, Paris, France, July 1-4, 2020, Proceedings, Part I*, volume 12166 of *Lecture Notes in Computer Science*, pages 375–394. Springer, 2020. doi:10.1007/978-3-030-51074-9\_21.
- [13] Simon Cruanes. Superposition with structural induction. In Clare Dixon and Marcelo Finger, editors, *Frontiers of Combining Systems - 11th International Symposium, FroCoS 2017, Brasília, Brazil, September 27-29, 2017, Proceedings*, volume 10483 of *Lecture Notes in Computer Science*, pages 172–188. Springer, 2017. doi:10.1007/978-3-319-66167-4\_10.
- [14] Mnacho Echenim and Nicolas Peltier. Combining induction and saturation-based theorem proving. *J. Autom. Reason.*, 64(2):253–294, 2020. doi:10.1007/s10817-019-09519-x.
- [15] Stephan Falke and Deepak Kapur. Rewriting induction + linear arithmetic = decision procedure. In Bernhard Gramlich, Dale Miller, and Uli Sattler, editors, *Automated Reasoning*, volume 7364 of *LNCS*, pages 241–255. Springer Berlin Heidelberg, 2012. URL: [http://dx.doi.org/10.1007/978-3-642-31365-3\\_20](http://dx.doi.org/10.1007/978-3-642-31365-3_20), doi:10.1007/978-3-642-31365-3\_20.
- [16] Jürgen Giesl and Deepak Kapur. Decidable classes of inductive theorems. In Rajeev Goré, Alexander Leitsch, and Tobias Nipkow, editors, *IJCAR*, volume 2083 of *LNCS*, pages 469–484. Springer, 2001.



- [17] Márton Hajdú, Petra Hozzová, Laura Kovács, and Andrei Voronkov. Induction with recursive definitions in superposition. In *Formal Methods in Computer Aided Design, FMCAD 2021, New Haven, CT, USA, October 19-22, 2021*, pages 1–10. IEEE, 2021. doi:10.34727/2021/isbn.978-3-85448-046-4\\_34.
- [18] Artur Jez. Deciding context unification. *J. ACM*, 66(6):39:1–39:45, 2019. doi:10.1145/3356904.
- [19] K. Rustan M. Leino and Michal Moskal. Co-induction simply - automatic co-inductive proofs in a program verifier. In Cliff B. Jones, Pekka Pihlajasaari, and Jun Sun, editors, *FM 2014: Formal Methods - 19th International Symposium, Singapore, May 12-16, 2014. Proceedings*, volume 8442 of *Lecture Notes in Computer Science*, pages 382–398. Springer, 2014. doi:10.1007/978-3-319-06410-9\\_27.
- [20] A. Leitsch. *The resolution calculus*. Springer. Texts in Theoretical Computer Science, 1997.
- [21] Dorel Lucanu and Grigore Rosu. CIRC : A circular coinductive prover. In Till Mossakowski, Ugo Montanari, and Magne Haveraaen, editors, *Algebra and Coalgebra in Computer Science, Second International Conference, CALCO 2007, Bergen, Norway, August 20-24, 2007, Proceedings*, volume 4624 of *Lecture Notes in Computer Science*, pages 372–378. Springer, 2007. doi:10.1007/978-3-540-73859-6\\_25.
- [22] Michael J. Maher. Complete axiomatizations of the algebras of finite, rational and infinite trees. In *Proceedings of the Third Annual Symposium on Logic in Computer Science (LICS '88), Edinburgh, Scotland, UK, July 5-8, 1988*, pages 348–357. IEEE Computer Society, 1988.
- [23] Alberto Momigliano and Alwen Fernanto Tiu. Induction and co-induction in sequent calculus. In Stefano Berardi, Mario Coppo, and Ferruccio Damiani, editors, *Types for Proofs and Programs, International Workshop, TYPES 2003, Torino, Italy, April 30 - May 4, 2003, Revised Selected Papers*, volume 3085 of *Lecture Notes in Computer Science*, pages 293–308. Springer, 2003. doi:10.1007/978-3-540-24849-1\\_19.
- [24] Andrew Reynolds and Viktor Kuncak. *Verification, Model Checking, and Abstract Interpretation: 16th International Conference, VMCAI 2015, Mumbai, India, January 12-14, 2015. Proceedings*, chapter Induction for SMT Solvers, pages 80–98. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015. URL: [http://dx.doi.org/10.1007/978-3-662-46081-8\\_5](http://dx.doi.org/10.1007/978-3-662-46081-8_5), doi:10.1007/978-3-662-46081-8\_5.
- [25] Davide Sangiorgi. *Introduction to Bisimulation and Coinduction*. Cambridge University Press, 2012. URL: <http://www.worldcat.org/isbn/9781107003637>.
- [26] Luke Simon, Ajay Bansal, Ajay Mallya, and Gopal Gupta. Co-logic programming: Extending logic programming with coinduction. In Lars Arge, Christian Cachin, Tomasz Jurdzinski, and Andrzej Tarlecki, editors, *Automata, Languages and Programming, 34th International Colloquium*,

*ICALP 2007, Wroclaw, Poland, July 9-13, 2007, Proceedings*, volume 4596 of *Lecture Notes in Computer Science*, pages 472–483. Springer, 2007.