Implementing Inequality and Nondeterministic Specifications with Bi-rewriting Systems*

Jordi Levy and Jaume Agustí

Institut d'Investigació en Intel·ligència Artificial, CSIC,
Camí Sta. Bàrbara s/n, 17300 Blanes, Girona, Spain.
E-mail: levy@ceab.es and agusti@ceab.es

Abstract. Rewriting with non-symmetric relations can be considered as a computational model of many specification languages based on non-symmetric relations. For instance, Logics of Inequalities, Ordered Algebras, Rewriting Logic, Order-Sorted Algebras, Subset Logic, Unified Algebras, taxonomies, subtypes, Refinement Calculus, all them use some kind of non-symmetric relation on expressions. We have developed an operational semantics for these inequality specifications named bi-rewriting systems. In this paper we show the applicability of bi-rewriting systems to Unified Algebras and nondeterministic specifications. In the first case, we give a canonical bi-rewriting system implementing the basic theory of these algebras. In the second case, nondeterministic specifications are viewed as inclusion specifications, thus bi-rewriting is a sound, although not always complete deduction method. We show how a specification has to be completed in order to have both soundness and completeness.

1 Introduction

Term rewriting systems TRS have been usually associated with equational logic [DJ90]. Overcoming this tendency it has been shown recently [Mes90, Mes92] that the logic implicit in TRS is a generalization of equational logic, named *preorder logic* POL, or rewriting logic, which is addressed to unify a wide variety of models of concurrency. Following the new trend, we proposed in [LA93] an operative method based on rewriting techniques to automatize the deduction in the preorder logic. The inference rules defining this logic are quite similar to the ones defining the equational logic, but they do not include the symmetry rule:

$$\frac{}{t \subseteq t} \; \textit{Reflexivity} \qquad \frac{s \subseteq t \quad t \subseteq v}{s \subseteq v} \; \textit{Transitivity}$$

$$\frac{s_1 \subseteq t_1 \; \dots \; s_n \subseteq t_n}{f(s_1,\dots,s_n) \subseteq f(t_1,\dots,t_n)} \; \textit{Monotonicity} \qquad \frac{s \subseteq t}{\sigma(s) \subseteq \sigma(t)} \; \textit{Substitution}$$

* This work has been partially supported by the project TESEU (TIC 91-430) funded by the CICYT.

An inclusion theory or specification I is defined by a finite set of inclusions $t \subseteq u$, where t and u are first order terms $\mathcal{T}(\Sigma, \mathcal{X})$ over a finite signature $\Sigma = \cup_{n \geq 0} \Sigma^n$ of function symbols and a denumerable set of variables $\mathcal{X}$.

The idea of applying rewriting techniques to the deduction of inclusions between terms like $t \subseteq u$ is very simple. We compute by repeatedly replacing both 1) subterms of t by *bigger* terms using the axioms and 2) subterms of u by *smaller* terms using the same axioms, until we find a path of the bi-directional search connecting t and u. To use inclusion axioms as rewrite rules we must orient them in one, the other or both directions, which produces a pair of rewriting system: one $R_{\subseteq}$ with rules oriented like $t \xrightarrow{\subseteq} u$ and the other $R_{\supseteq}$ with rules like $u \xrightarrow{\supseteq} t$. The pair $\langle R_{\subseteq}, R_{\supseteq} \rangle$ is a bi-rewriting system.

In [LA93] we started to study the theory of bi-rewriting systems, their properties and the completion process in order to ensure the termination and completeness of the bi-directional search proof procedure. These depend on two properties, the termination of both rewriting relations $\xrightarrow[R_{\subseteq}]{}$ and $\xrightarrow[R_{\supseteq}]{}$, and the commutation of them $\xleftarrow[R_{\supseteq}]{} \circ \xrightarrow[R_{\subseteq}]{} \subseteq \xrightarrow[R_{\subseteq}]{*} \circ \xleftarrow[R_{\supseteq}]{*}$. The first property is usually proved using the standard methods based on simplification orderings. The second one requires a new definition:

Definition 1. Let $\alpha_1 \xrightarrow{\subseteq} \beta_1$ in $R_{\subseteq}$ and $\alpha_2 \xrightarrow{\supseteq} \beta_2$ in $R_{\supseteq}$ be two rewriting rules (with distinct variables) and p a position in α_1, then

1. if $\alpha_1|_p$ is a non-variable subterm and ρ is the most general unifier of $\alpha_1|_p$ and α_2 then $\rho(\alpha_1[\beta_2]_p) \subseteq \rho(\beta_1)$ is a *(standard) critical pair*,
2. if $\alpha_1|_p = x$ is a repeated variable in α_1, F a term, q an occurrence in F, and $\alpha_2 \xrightarrow[R_{\subseteq}]{*} \beta_2$ is not satisfied, then $\rho(\alpha_1[F[\beta_2]_q]_p) \subseteq \rho(\beta_1)$ is an *(extended) critical pair* where ρ only substitutes x by $F[\alpha_2]_q$.

The same for critical pairs between $R_{\supseteq}$ and $R_{\subseteq}$.

In [LA93] we proved the following theorem.

Theorem 2. *Given a bi-rewriting system $\langle R_{\subseteq}, R_{\supseteq} \rangle$, if $R_{\subseteq}$ and $R_{\supseteq}$ are both terminating then the bi-rewriting system commutes iff all the critical pairs are confluent.*

The same result was extended to bi-rewriting modulo a set of nonorientable inclusions, like it is done in the equational case when we rewrite in equivalence classes. The Knuth-Bendix completion process for bi-rewriting systems has some problems (the set of extended critical pairs is in general infinite) which are the object of current work [Lev93].

In this paper we apply the bi-rewriting technique to the automatic deduction in inclusion specifications. In section 2 we complete the basic inclusion theory of Unified Algebras, that is the theory of distributive lattices, and we give a canonical bi-rewriting system for it. This example shows the problems arising from the use of extended critical pairs.

Section 3 has more theoretical interest. It has been shown that bi-rewriting is a sound and complete deduction technique for the preorder logic. The class of models of this logic are the preorder algebras. However, the models usually used in nondeterministic specifications are multialgebras. We study which conditions a specification I has to satisfy in order to be equivalent both classes of models. If this conditions are not satisfied, we propose a completion method for I. This completion introduces new rules $t \xrightarrow{\subseteq} u$, leaving the rules $t \xrightarrow{\supseteq} u$ which define the computation unchanged.

2 Implementing the Inequality Specification of Distributive Lattices

The commutativity of a bi-rewriting system requires the confluence of all the standard and extended critical pairs. The confluence of a standard critical pair, like $l \subseteq r$, can be assured adding to the system the rule $l \xrightarrow{\subseteq} r$ or $r \xrightarrow{\supseteq} l$ when it is not confluent. The same solution does not apply to the extended critical pair case because they involve inclusion schemes. The confluence of an inclusion scheme may require the addition of more than one rule and the search of the rules to add is not automatizable. Our approach to the problem is to orient the inclusion scheme in a rule scheme, and to study the new rule schemes that can be generated from it. The generation of critical pairs between rule schemes has not been solved yet. Nevertheless, in the following example we show that some particular rule instances of rule schemes may make confluent the original inclusion scheme (the extended critical pair). The rules added are sound because they are instances of rule schemes generated from extended critical pairs.

The example we present is the inequality specification of distributive lattices. This specification is the base for many other specifications or specification languages like the *Unified Algebras* [Mos89]. The presentation of the distributive lattice theory may be given by the following set of inclusions:

$$
\begin{array}{ll}
X \cup X \subseteq X & X \cap X \supseteq X \\
X \cup Y \supseteq X & X \cap Y \subseteq X \\
X \cup Y \supseteq Y & X \cap Y \subseteq Y \\
\multicolumn{2}{c}{X \cap (Y \cup Z) \subseteq (X \cap Y) \cup (X \cap Z)}
\end{array}
$$

The orientation of all these inclusions to the right results in a terminating bi-rewriting system where all *standard* critical pairs are confluent. However, the presence of the two non-left-linear rules $X \cup X \xrightarrow{\subseteq} X$ and $X \cap X \xrightarrow{\supseteq} X$ makes necessary the consideration of the *extended* critical pairs. If we only take into account, in a first step, all those extended critical pairs of the form $\langle \sigma(\alpha_1[\beta_2]_p), \sigma(\beta_1) \rangle$, which correspond to the particular case where the position q in F is the most external one $q = \lambda$, then we can generate the following sequence of new rules:

q_1 $Y \cup (X \cup Y) \xrightarrow{\subseteq} X \cup Y$
q_2 $Y \cup X \xrightarrow{\subseteq} X \cup Y$

q_3 $(X \cup Y) \cup Y \xrightarrow{\subseteq} X \cup Y$
q_4 $(X \cup Y) \cup (Y \cup Z) \xrightarrow{\subseteq} X \cup (Y \cup Z)$
q_5 $(X \cup Y) \cup Z \xrightarrow{\subseteq} X \cup (Y \cup Z)$

and the equivalent ones for $\cap$. The rules q_2 and q_5 are non-orientable and subsume the rest of rules. They make necessary the use of the bi-rewriting modulo a set of inclusions technique. These rules are symmetric –they are really equations–, therefore we can apply the standard commutative-associative closure definition [PS81]. We obtain then the following set of rules.

$$R_{\subseteq} = \begin{cases} r_1 & X \cup X \xrightarrow{\subseteq} X \\ r_1^{ext} & X \cup X \cup Y \xrightarrow{\subseteq} X \cup Y \\ r_2 & X \cap Y \xrightarrow{\subseteq} X \\ r_3 & X \cap (Y \cup Z) \xrightarrow{\subseteq} (X \cap Y) \cup (X \cap Z) \\ r_3^{ext} & X \cap (Y \cup Z) \cap T \xrightarrow{\subseteq} \Big((X \cap Y) \cup (X \cap Z)\Big) \cap T \end{cases}$$

$$R_{\supseteq} = \begin{cases} r_4 & X \cap X \xrightarrow{\supseteq} X \\ r_4^{ext} & X \cap X \cap Y \xrightarrow{\supseteq} X \cap Y \\ r_5 & X \cup Y \xrightarrow{\supseteq} X \end{cases}$$

$$I = \begin{cases} r_6 \; Y \cup X \xrightarrow{\subseteq} X \cup Y \\ r_7 \; (X \cup Y) \cup Z \xrightarrow{\subseteq} X \cup (Y \cup Z) \\ r_8 \; Y \cap X \xrightarrow{\subseteq} X \cap Y \\ r_9 \; (X \cap Y) \cap Z \xrightarrow{\subseteq} X \cap (Y \cap Z) \end{cases}$$

In a second step we have to consider also those rules needed to make confluent the rest of extended critical pairs.

$$F[X] \cup F[X \cup Y] \subseteq F[X \cup Y]$$
$$F[X \cap Y] \subseteq F[X] \cap F[X \cap Y]$$

First, we will study the second extended critical pair. If we orient it to the left, we obtain the rule scheme $F[X] \cap F[X \cap Y] \xrightarrow{\supseteq} F[X \cap Y]$. This rule scheme generates a standard critical pair with the rule $X \cap Y \xrightarrow{\subseteq} Y$, which is made confluent adding the rule scheme $F[X] \cap F[Y] \xrightarrow{\supseteq} F[X \cap Y]$. The overlapping of the context $F[\_]$ of this rule scheme with the left part of the rule $X \cap Y \xrightarrow{\subseteq} Y$ generates infinite many rule schemes $F[X_1, \ldots, X_n] \cap F[Y_1, \ldots, Y_n] \xrightarrow{\supseteq} F[X_1 \cap Y_1, \ldots, X_n \cap Y_n]$ for $n \geq 1$. The following (normal) rules subsume these rule schemes.

r_{10} $X \cap (Y \cup Z) \xrightarrow{\supseteq} (X \cap Y) \cup (X \cap Z)$
$r_{11}^{(f)}$ $f(X_1, \ldots, X_n) \cap f(Y_1, \ldots, Y_n) \xrightarrow{\supseteq} f(X_1 \cap Y_1, \ldots, X_n \cap Y_n)$ $\forall f \in \Sigma^n$

Notice that $r_{11}^{(f)}$ is really a set of rules, one for each n-ary symbol $f \in \Sigma^n$, and that r_{10} subsumes the instantiation of $r_{11}^{(f)}$ for the symbol $\cup \in \Sigma^2$.

The dual solution is not applicable to $F[X] \cup F[X \cup Y] \subseteq F[X \cup Y]$ because $X \cup (Y \cap Z) \xrightarrow{\subseteq} (X \cup Y) \cap (X \cup Z)$ and the distributive rule r_3 would lead to the non-termination of the system. This problem can be avoided using the alternative set of rules:

$$\begin{array}{ll} r_{12}^{(f)} & f(X_1,\dots,X_n)\cup f(Y_1,\dots,Y_n)\xrightarrow{\subseteq} f(X_1\cup Y_1,\dots,X_n\cup Y_n)\\ r_{13}^{(f)} & \big(X\cap f(Y_1,\dots,Y_n)\big)\cup\big(X\cap f(Z_1,\dots,Z_n)\big)\xrightarrow{\subseteq}\\ & \qquad\xrightarrow{\subseteq} X\cap f(Y_1\cup Z_1,\dots,Y_n\cup Z_n)\end{array}$$

They do not subsume $F[X]\cup F[Y]\xrightarrow{\subseteq}F[X\cup Y]$, but are particular instances of this rule schema. The last rule r_{13} is non-left-linear and generates a new extended critical pair which becomes confluent if we add the following rule.

$$\begin{array}{ll} r_{14}^{(f)} & \big(X\cap f(Y_1,\dots,Y_n)\big)\cup\big(Z\cap f(V_1,\dots,V_n)\big)\xrightarrow{\subseteq}\\ & \qquad\xrightarrow{\subseteq}(X\cup Z)\cap f(Y_1\cup V_1,\dots,Y_n\cup V_n)\end{array}$$

Rules $r_{14}^{(f)}$ and r_1 subsume $r_{13}^{(f)}$.

Let's prove now that rules r_{12} and r_{14} makes confluent the extended critical pair $F[X]\cup F[X\cup Y]\subseteq F[X\cup Y]$. Rules $r_{12}^{(f)}$ and $r_{14}^{(f)}$ subsume $F[X]\cup F[Y]\xrightarrow{\subseteq}F[X\cup Y]$ when the schema[2] $F[\_]$ can be expressed as a composition $F[\_]=F_1[\dots F_n[\_]\dots]$ of schemas, where each one of this schemes satisfies $F_i[\_]=f(\dots,\_,\dots)$, or $F_i[\_]=E_1\cap f(\dots,\_,\dots)\cap E_2$ for any symbol f different from $\cap$, and any expressions E_1,E_2. It can be proved that any scheme $F[\_]$ can be expressed as $F[\_]=G[E_1\cap\_\cap E_2]$ where the schema $G[\_]$ satisfies the previous condition and E_1,E_2 are two common expressions. This property allows to translate the inclusion schema (the extended critical pair) $F[X]\cup F[X\cup Y]\subseteq F[X\cup Y]$ into

$$G[X\cap H]\cup G[(X\cup Y)\cap H]\subseteq G[(X\cup Y)\cap H]$$

where $G[\_]$ can be rewritten using $F[X]\cup F[Y]\xrightarrow{\subseteq}F[X\cup Y]$. We prove then that this extended critical pair is bi-confluent using the following proof.

$$\begin{array}{rl} G[X\cap H]\cup G[(X\cup Y)\cap H] & \xrightarrow{\subseteq} G\big[(X\cap H)\cup\big((X\cup Y)\cap H\big)\big]\\ & \xrightarrow{\subseteq} G[(X\cap H)\cup(X\cap H)\cup(Y\cap H)]\\ & \xrightarrow{\subseteq} G[(X\cap H)\cup(Y\cap H)]\xleftarrow{\subseteq}G[(X\cup Y)\cap H]\end{array}$$

A commutative and terminating bi-rewriting system for the distributive lattice theory is given by rules $r_1\dots r_{12}$, r_{14} and their corresponding $\cup$ and $\cap$ associative-commutative extensions.

3 Implementing Nondeterministic Specifications

It is well known that term rewriting techniques can be used to test the equivalence of terms in a equational logic specification E. The method consists in finding the normal form of both sides of the tested equality and checking if they are equal. The method is sound and complete for ground terms if the set

[2] As usual, an schema is an expression with a *hole* in it, a selected position, denoted by an underscore "_". The schema composition $F[\_]\circ G[\_]$ is defined by the substitution of this selected position by the other schema, noted $F[G[\_]]$.

of ground normal forms is (isomorphic to) the initial model of the specification; and for terms with variables if the set of normal forms is isomorphic to $\mathcal{T}(\Sigma, \mathcal{X})/E$ [DJ90]. It is also well known that the confluence and termination of the rewriting system resulting from orienting the equations is a sufficient condition for this completeness result.

Term rewriting techniques have also been proposed as the implementation language of nondeterministic specifications [Kap86a, Hus92]. In all these approaches the signature includes a nondeterministic choice operator —noted by $\uparrow$ in [Kap86a, Kap88], by $or(\_,\_)$ in [Hus91, Hus92], or by $\cup$ in our work— which makes nondeterministic computation lose the symmetry property. Otherwise, the rules $X \cup Y \longrightarrow X$ and $X \cup Y \longrightarrow Y$ proposed for the choice operator would allow to prove the equivalence of any two terms. Therefore, the confluence property makes no sense, and a nondeterministic specification is presented in general as a set of (non symmetric) inclusions.

The models proposed for these specifications are based on Σ-multialgebras [Hes88, Nip86], which capture the essence of nondeterminism better than the Σ-algebras used in equational specifications.

Definition 3. A Σ-multialgebra A is a tuple $\langle S^A, \mathcal{F}^A \rangle$ where S^A is a non empty carrier set, and $\mathcal{F}^A$ is a set of set-valued functions $f^A : S^A \times \overset{n}{\cdots} \times S^A \to \mathcal{P}^+(S^A)$ for each $f \in \Sigma^n$ function symbol of the signature.

Models are defined as follows.

Definition 4. Given a specification I over a signature Σ, a Σ-multialgebra A is said to be a model of I, noted $A \in MAlg(I)$, if the interpretation function $I^A_{\_}[\_] : (\mathcal{X} \to S^A) \to \mathcal{T}(\Sigma, \mathcal{X}) \to \mathcal{P}^+(S^A)$ defined inductively by

$$\begin{array}{lll} I^A_\rho[x] & = \{\rho(x)\} & \text{for any } x \in \mathcal{X} \\ I^A_\rho[f(t_1, \ldots, t_n)] & = \bigcup\{f^A(v_1, \ldots, v_n) \mid v_i \in I^A_\rho[t_i]\} & \text{for any } f \in \Sigma^n \end{array}$$

satisfies $I^A_\rho[t] \subseteq I^A_\rho[u]$ for any axiom $t \subseteq u$ in the specification I, and any valuation function $\rho : \mathcal{X} \to S^A$.

An inclusion $t \subseteq u$ is valid in a Σ-multialgebra model A, noted $A \models t \subseteq u$, if for any valuation ρ we have $I^A_\rho[t] \subseteq I^A_\rho[u]$.

3.1 Using Bi-rewriting Systems to Verify Specifications

Bi-rewriting systems introduced in [LA93] automatize the deduction in the *Partial Order Logic* POL (also for the rewriting logic of Meseguer [Mes92]). The models of this logic are preorder algebras, defined as follows.

Definition 5. A Σ-preorder algebra A is a triplet $\langle S^A, \subseteq_A, \mathcal{F}^A \rangle$ where S^A is a carrier set, $\subseteq_A$ is a preorder relation and $\mathcal{F}^A$ is a set of monotonic functions $f^A : S^A \times \overset{n}{\cdots} \times S^A \to S^A$ for each symbol $f \in \Sigma^n$.

Definition 6. Given a specification I over Σ a Σ-preorder algebra A is said to be a model of I, noted $A \in \mathit{POAlg}(I)$, if the interpretation function $I_{\_}^{A}[\_] : (\mathcal{X} \to S^A) \to \mathcal{T}(\Sigma, \mathcal{X}) \to S^A$ defined inductively by

$$\begin{array}{lll} I_\rho^A[x] & = \rho(x) & \text{for any } x \in \mathcal{X} \\ I_\rho^A[f(t_1, \dots, t_n)] & = f^A(I_\rho^A[t_1], \dots, I_\rho^A[t_n]) & \text{for any } f \in \Sigma^n \end{array}$$

satisfies $I_\rho[t] \subseteq_A I_\rho[u]$ for any axiom $t \subseteq u$ in the specification I and any valuation $\rho : \mathcal{X} \to S^A$.

A soundness and completeness theorem, similar to the Birkhoff theorem, can be stated for this logic.

Lemma 7. *For any specification I and any pair of terms t and u we have $\mathit{POAlg}(I) \models t \subseteq u$ iff $I \vdash_{\mathit{POL}} t \subseteq u$.*

Commutative and terminating bi-rewriting systems automatize the deduction in $\vdash_{\mathit{POL}}$. They are a sound and complete method w.r.t. the semantics of specifications based on preorder algebras. However, $\mathit{POAlg}(I) \models t \subseteq u$ and $\mathit{MAlg}(I) \models t \subseteq u$ are not equivalent (the implication does not hold in none of both directions) as the following counter-example shows.

Example 1. A counter-example to $\mathit{MAlg}(I) \models t \subseteq u \Rightarrow \mathit{POAlg}(I) \models t \subseteq u$ is given by the following additivity axiom which is sound in multialgebra models, but not in preorder algebra models.

$$\frac{}{f(X \cup Y) \subseteq f(X) \cup f(Y)} \; \mathit{Aditivity}$$

The counter-example to $\mathit{POAlg}(I) \models t \subseteq u \Rightarrow \mathit{MAlg}(I) \models t \subseteq u$ is not so evident, and causes more problems. The following substitution rule is sound in preorder models, but not in multialgebra models, in the presence of repeated variables.

$$\frac{t \subseteq u}{\sigma(t) \subseteq \sigma(u)} \; \mathit{Substitution}$$

For instance, the deduction

$$f(X, X) \subseteq g(X) \; , \; X \subseteq X \cup Y \; , \; Y \subseteq X \cup Y \; \vdash_{\mathit{POL}} \; f(X, Y) \subseteq g(X \cup Y)$$

is correct in POL. However, it is not sound in a multialgebra model. The multialgebra $A = \langle S^A, \mathcal{F}^A \rangle$ defined by:

$$S^A = \{a, b\} \qquad \begin{array}{ll} f^A(x, y) & = if \ x = y \ then \ \{a\} \ else \ \{b\} \\ g^A(x, y) & = \{a\} \\ x \cup^A y & = \{x, y\} \end{array}$$

is a model of $I = \{f(X, X) \subseteq g(X), X \subseteq X \cup Y, Y \subseteq X \cup Y\}$, however $I_\rho^A[f(X, Y)] \not\subseteq I_\rho^A[g(X \cup Y)]$ for $\rho = [a \leftarrow X, b \leftarrow Y]$.

We understand variables in a specification denoting terms and being universally quantified. Therefore, we think that the substitution rule has to be sound in any specification model. Multialgebra models may satisfy this requirement if we modify the definition of interpretation and model:

Definition 8. A Σ-multialgebra A is said to be a *strong* model of a specification I, noted $A \in \overline{MAlg}(I)$, if the interpretation function $I^A_{\_}[\_] : (\mathcal{X} \to \mathcal{P}^+(S^A)) \to \mathcal{T}(\Sigma, \mathcal{X}) \to \mathcal{P}^+(S^A)$ defined inductively by

$$\begin{array}{lll} I^A_\rho[x] & = \rho(x) & \text{for any } x \in \mathcal{X} \\ I^A_\rho[f(t_1, \ldots, t_n)] & = \bigcup\{f^A(v_1, \ldots, v_n) \mid v_i \in I^A_\rho[t_i]\} & \text{for any } f \in \Sigma^n \end{array}$$

satisfies $I_\rho[t] \subseteq I_\rho[u]$ for any axiom $t \subseteq u$ in the specification I, and any valuation $\rho : \mathcal{X} \to \mathcal{P}^+(S^A)$.

Notice that the valuation function ρ ranges over sets and not only over values.

Lemma 9. *For any specification I we have $\overline{MAlg}(I) \subseteq MAlg(I)$.*

Using this smaller class of models the preorder logic entailment $\vdash_{POL}$ becomes sound.

Theorem 10. *If $POAlg(I) \models t \subseteq u$ holds, then $\overline{MAlg}(I) \models t \subseteq u$ also holds. Therefore, bi-rewriting is a sound deduction method.*

Proof. It is sufficient to prove that

$$\forall A \in \overline{MAlg} \,.\, \exists B \in POAlg \,.\, (\forall \rho \,.\, I^A_\rho[t] \subseteq I^A_\rho[u]) \Leftrightarrow (\forall \rho' \,.\, I^B_{\rho'}[t] \subseteq_B I^B_{\rho'}[u])$$

Notice that we use one implication direction to prove $A \in \overline{MAlg}(I) \Rightarrow B \in POAlg(I)$, and the opposite direction to prove $B \models t \subseteq u \Rightarrow A \models t \subseteq u$.

Any Σ-multialgebra A has a Σ-preorder algebra B naturally associated. This preorder algebra B is defined by

$$\begin{array}{l} S^B \stackrel{def}{=} \mathcal{P}^+(S^A) \\ f^B(s_1, \ldots, s_n) \stackrel{def}{=} \bigcup\{f^A(v_1, \ldots, v_n) \mid v_i \in s_i\} \text{ for any } f \in \Sigma^n \end{array}$$

The carrier S_B is a power set, and the set inclusion relation $\subseteq$ used in the multialgebra model A, and the partial order relation $\subseteq_B$ used in the preorder model B are equal. We can prove by structural induction on the term t that $I^A_\rho[t] = I^B_\rho[t]$.

$$\begin{array}{rl} I^B_\rho[x] & = \rho(x) = I^A_\rho[x] \\ I^B_\rho[f(t_1 \ldots t_n)] & = f^B(I^B_\rho[t_1] \ldots I^B_\rho[t_n]) = \bigcup\{f^A(v_1 \ldots v_n) \mid v_i \in I^B_\rho[t_i]\} \\ & = \bigcup\{f^A(v_1 \ldots v_n) \mid v_i \in I^A_\rho[t_i]\} = I^A_\rho[f(t_1 \ldots t_n)] \end{array}$$

Then the initial double implication becomes a tautology.

In the following we will study which conditions I has to satisfy in order to be $POAlg(I) \models t \subseteq u$ and $\overline{MAlg}(I) \models t \subseteq u$ equivalent.

Theorem 11. *If the specification I satisfies:*

1. *I contains the union theory as a subtheory:*
   $I \vdash_{POL} X \cup X \subseteq X,\ X \subseteq X \cup Y,\ Y \subseteq X \cup Y.$
2. $I \vdash_{POL} t = \cup\{u \in Atomic(I) \mid I \vdash_{POL} u \subseteq t\}$, *for any term t, where* $Atomic(I) \stackrel{def}{=} \{u \in \mathcal{T}(\Sigma, \mathcal{X}) \mid$ *if* $I \vdash_{POL} v \subseteq u$ *then* $v = u\}$.
3. $I \vdash_{POL} f(\ldots t \cup u \ldots) \subseteq f(\ldots t \ldots) \cup f(\ldots u \ldots)$ *for any n-ary symbol* $f \in \Sigma^n$.
4. *If $t \in Atomic(I)$ and $I \vdash_{POL} t \subseteq u \cup u'$ then either $I \vdash_{POL} t \subseteq u$ or $I \vdash_{POL} t \subseteq u'$.*

Then, whenever $\overline{MAlg}(I) \models t \subseteq u$ holds, then $POAlg(I) \models t \subseteq u$ also holds. Therefore, bi-rewriting is a complete deduction method for these specifications.

Proof. It is sufficient to prove that

$$\forall B \in POAlg\,.\,\exists A \in \overline{MAlg}\,.\,(\forall \rho\,.\,I^A_\rho[t] \subseteq I^A_\rho[u]) \Leftrightarrow (\forall \rho'\,.\,I^B_{\rho'}[t] \subseteq_B I^B_{\rho'}[u])$$

We can also associate a multialgebra A to each preorder algebra B as follows.

$$S^A \stackrel{def}{=} Atomic(S^B)$$
$$f^A(v_1, \ldots, v_n) \stackrel{def}{=} \{s \in S^A \mid s \subseteq_B f^B(v_1, \ldots, v_n)\} \text{ for any } f \in \Sigma^n$$

where for any preorder S, we define $Atomic(S) \stackrel{def}{=} \{s \in S \mid s' \subseteq s \Rightarrow s = s'\}$.[3]

Notice that in this case $\subseteq$ is the set inclusion in $\mathcal{P}^+(S^B)$, and $\subseteq_B$ is a preorder relation on S^B, and they are different relations.

Case $\forall \rho'\,.\,\exists \rho\,.\,I^A_\rho[t] \subseteq I^A_\rho[u] \Rightarrow I^B_{\rho'}[t] \subseteq_B I^B_{\rho'}[u]$.

The conditions of the theorem can be translated directly to properties of the preorder algebra B:

$$v \cup^B v \subseteq_B v \quad v_1 \subseteq_B v_1 \cup^B v_2 \quad v_2 \subseteq_B v_1 \cup^B v_2$$
$$f^B(\ldots v_1 \cup^B v_2 \ldots) \subseteq_B f^B(\ldots v_1 \ldots) \cup^B f^B(\ldots v_2 \ldots)$$
$$v = \cup^B\{v' \in Atomic(S^B) \mid v' \subseteq_B v\}$$
$$v \in Atomic(S^B) \ \wedge\ v \subseteq v_1 \cup v_2 \ \Rightarrow\ v \subseteq v_1 \ \vee\ v \subseteq v_2$$

If we define $\rho(x) \stackrel{def}{=} \{s \in S^A \mid s \subseteq_B \rho'(x)\}$ then using the properties below we can prove by structural induction on the term t that

$$I^B_{\rho'}[t] = \cup^B I^A_\rho[t]$$

where, as usual $\cup^B\{v_1, \ldots, v_n\} = v_1 \cup^B \cdots \cup^B v_n$ for any $v_1 \ldots v_n \in S^B$. Then the monotonicity of $\cup^B$ proves that $I^A_\rho[t] \subseteq I^A_\rho[u]$ implies $I^B_{\rho'}[t] \subseteq I^B_{\rho'}[u]$.

[3] Notice that for the free algebra of terms $\mathcal{T}(\Sigma, \mathcal{X})/I$ this definition and the previous one becomes equivalent.

Case $\forall \rho \,.\, \exists \rho' \,.\, I^B_{\rho'}[t] \subseteq_B I^B_{\rho'}[u] \Rightarrow I^A_\rho[t] \subseteq I^A_\rho[u]$.

The last two conditions of the theorem prove that if $t \in \mathit{Atomic}(I)$ and $I \vdash_{\scriptscriptstyle POL} t \subseteq f(u_1, \ldots, u_n)$ then there exist $v_1, \ldots, v_n \in \mathit{Atomic}(I)$ such that $I \vdash_{\scriptscriptstyle POL} t \subseteq f(v_1, \ldots, v_n)$ for any $f \in \Sigma^n$.

If we define $\rho'(x) = \cup^B \rho(x)$ then we can prove

$$I^A_\rho[t] = \{s \in S^A \mid s \subseteq_B I^B_{\rho'}[t]\}$$

for any term t by structural induction.

Then $I^B_{\rho'}[t] \subseteq_B I^B_{\rho'}[u]$ implies $I^A_\rho[t] \subseteq I^A_\rho[u]$.

The conditions of the previous theorem are usually satisfied in any nondeterministic specification I. We will find the same conditions in the next subsection where we try to prove the existence and initiality of a model based on sets of normal forms.

3.2 Characterizing Terms by Sets of Normal Forms

In nondeterministic computations terms can not be characterized by a unique normal form, but we will try to characterize them by its set of normal forms. In this case, a method to test inclusions of terms in a nondeterministic specification would consist in searching the set of normal forms of each side of the inclusion, and checking if one set is included in the other one. We will prove that the soundness and completeness of this *nondeterministic computation* method relies on the existence and initiality of a model of *set of normal forms* –like in the equational case with the normal form model–. The main goal of this section is to give the conditions for the existence and for the initially of this model –like it is characterized in the equational case by the confluence and termination properties–.

First we will present the formal definition of the *set of normal forms* model, SNF-model for short, and later we will study the *nondeterministic computation* method, NDC-method for short.

Nondeterministic computation is based on the computation of normal forms only using the rewriting system $R_\supseteq$. As we will see, the other rewriting system $R_\subseteq$ does not play a computational role, but its rules may be understood as semantic constraints on the class of models of the specification. The example at the end of the section shows this clearly. Adding new rules to $R_\subseteq$ we can prove a soundness and completeness result for the nondeterministic computation and the bi-rewriting methods w.r.t. the models of the new specification.

Given a rewriting system $R_\supseteq$, we will denote the set of its $R_\supseteq$-normal forms by $\mathit{NF}^\supseteq$ and the set of $R_\supseteq$-normal forms of a term t by $\mathit{NF}^\supseteq[t]$.

The *set of normal forms* multialgebra, SNF-multialgebra for short, is defined as follows.

Definition 12. Given a rewriting system $R_\supseteq$, the SNF-multialgebra $\mathit{SNF} = \langle S^{\mathit{SNF}}, \mathcal{F}^{\mathit{SNF}} \rangle$ is defined by the carrier set $S^{\mathit{SNF}} \stackrel{def}{=} \mathit{NF}^\supseteq$, and the set of functions $f^{\mathit{SNF}} : \mathit{NF}^\supseteq \times \stackrel{n}{\ldots} \times \mathit{NF}^\supseteq \to \mathcal{P}^+(\mathit{NF}^\supseteq)$ defined by $f^{\mathit{SNF}}(t_1, \ldots, t_n) = \mathit{NF}^\supseteq[f(t_1, \ldots, t_n)]$ for each functional symbol $f \in \Sigma^n$ of the signature.

Notice that the SNF-multialgebra is defined syntactically using $R_{\supseteq}$, and independently of I. The rewriting rules of $R_{\supseteq}$ come from the orientation of some of the axioms of I. However, this fact is not enough to prove that the SNF-multialgebra is a multialgebra model of I.

Lemma 13. *Given a specification I and a rewriting system $R_{\supseteq}$, if the following conditions hold.*

1. *For any inclusion $t \subseteq u$ in I, and any substitution $\rho : \mathcal{X} \to NF^{\supseteq}$, we have $NF^{\supseteq}[\rho(t)] \subseteq NF^{\supseteq}[\rho(u)]$.*
2. *If $t \in NF^{\supseteq}[f(\ldots,u,\ldots)]$, then there exists $u' \in NF^{\supseteq}[u]$ such that $t \in NF^{\supseteq}[f(\ldots,u',\ldots)]$.*

then the SNF-multialgebra is a multialgebra model of I, $SNF \in MAlg(I)$, and the interpretation function is $I_{\rho}^{SNF}[t] = NF^{\supseteq}[\rho(t)]$.

Additionally, if the following condition also holds

3. *$NF^{\supseteq}[t \cup u] \subseteq NF^{\supseteq}[t] \cup NF^{\supseteq}[u]$,*

then the SNF-multialgebra is a strong multialgebra model of I, $SNF \in \overline{MAlg}(I)$, and $I_{\rho}^{SNF}[t] = NF^{\supseteq}[\rho'(t)]$, where for any $x \in \mathcal{X}$, $\rho'(x) = \cup\rho(x)$.

Proof. First we prove that $I_{\rho}^{SNF}[t] = NF^{\supseteq}[\rho(t)]$ are equal. That is, $NF^{\supseteq}[\rho(t)]$ satisfies the inductive definition of multialgebra interpretation function: 1) $I_{\rho}^{SNF}[x] = \rho(x)$ for any variable $x \in \mathcal{X}$. As far as ρ maps variables to normal forms, $NF^{\supseteq}[\rho(x)] = \{\rho(x)\}$. 2) $I_{\rho}^{SNF}[f(t_1,\ldots,t_n)] = \bigcup\{f^{SNF}(v_1,\ldots,v_n) \mid v_i \in I_{\rho}^{SNF}[t_i]\}$, which is equivalent to $NF^{\supseteq}[f(\rho(t_1),\ldots,\rho(t_n))] = \bigcup\{NF^{\supseteq}[f(v_1,\ldots,v_n)] \mid v_i \in NF^{\supseteq}[\rho(t_i)]\}$. The inclusion $\supseteq$ is always satisfied and it can be proved using the monotonicity of f. The inclusion $\subseteq$ is proved by the second condition of the lemma.

Second the first condition of the lemma and $I_{\rho}^{SNF}[t] = NF^{\supseteq}[\rho(t)]$ prove that $I_{\rho}^{SNF}[t] \subseteq I_{\rho}^{SNF}[u]$ for any inclusion $t \subseteq u$ of I, and any substitution ρ.

The proof of the second part of the lemma is quite similar. In this case we need the third condition to prove $I_{\rho}^{SNF}[t] = \rho(x) = NF^{\supseteq}[\cup\rho(x)] = NF^{\supseteq}[\rho'(x)]$.

As we have seen in the previous subsection we can associate a preorder algebra to the SNF-multialgebra, and this preorder algebra will be a preorder model of I if the SNF-multialgebra is a strong multialgebra model of I.

Lemma 14. *If the following conditions are satisfied:*

1. *If $I \vdash_{POL} t \subseteq u$ then $NF^{\supseteq}[t] \subseteq NF^{\supseteq}[u]$.*
2. *If $t \in NF^{\supseteq}[f(\ldots,u,\ldots)]$, then there exists $u' \in NF^{\supseteq}[u]$ such that $t \in NF^{\supseteq}[f(\ldots,u',\ldots)]$.*
3. *$NF^{\supseteq}[t \cup u] \subseteq NF^{\supseteq}[t] \cup NF^{\supseteq}[u]$,*

then, the SNF-preorder algebra defined by the carrier set $S^{SNF} \stackrel{def}{=} \mathcal{P}^{+}(NF^{\supseteq})$ and the set of functions $f^{SNF}(s_1 \ldots s_n) \stackrel{def}{=} \cup\{NF^{\supseteq}[f(v_1 \ldots v_n)] \mid v_i \in s_i\}$ is a preorder model of I.

If in addition

4. *If* $NF^{\supseteq}[t] \subseteq NF^{\supseteq}[u]$ *then* $I \vdash_{POL} t \subseteq u$.

then the SNF-preorder model is initial in $POAlg(I)$*, and the associated SNF-multialgebra is initial in* $\overline{MAlg}(I)$*.*

Moreover, $\overline{MAlg}(I) \models t \subseteq u$ *and* $POAlg(I) \models t \subseteq u$ *are equivalent.*

Proof. The proof of the first part of the lemma is a consequence of the previous lemma. The proof for the initiality of the model relies on the completeness of $\vdash_{POL}$ w.r.t. the class of models *POAlg*. The initiality of the model SNF w.r.t. the class $POAlg(I)$, and the fact that its associated multialgebra is a strong multialgebra model of I proves the last equivalence.

The conditions of this lemma reproduce the condition of theorem 11. Before reducing the four conditions of this lemma to syntactic conditions more easily provable, we will discuss its meaning.

The first condition $NF^{\supseteq}[t_1] \supseteq NF^{\supseteq}[t_2] \Rightarrow I \vdash_{POL} t_1 \supseteq t_2$ expresses the soundness of the NDC-method with respect to the specification. However, the user usually only gives the rewriting rules $R_{\supseteq}$, leaving the specification incomplete –as we will see in the examples–. This specification must be completed in order to verify this condition. Hence, we prefer to name this condition completeness of the specification with respect to the NDC-method.

The forth condition $I \vdash_{POL} t_1 \supseteq t_2 \Rightarrow NF^{\supseteq}[t_1] \supseteq NF^{\supseteq}[t_2]$ expresses the completeness of the method with respect to the specification. This condition is very easily satisfied. As it is noticed by Hussmann [Hus92] the more difficult point working with nondeterministic specifications is the soundness property of the method (or soundness of the Birkhoff theorem). Kaplan gives the theorem (theorem 2.3 in [Kap86a]) $MOD_R \models M = N$ iff $\{NF(M)\} = \{NF(N)\}$, although he does not use multialgebra models, and the theorem is stated in terms of equality, instead of inclusions.

The second property $t_2 \in NF^{\supseteq}[f(\ldots, t_1, \ldots)] \Rightarrow \exists t_3 \in NF^{\supseteq}[t_1] \,.\, t_2 \in NF^{\supseteq}[f(\ldots, t_3, \ldots)]$ is named additivity property. It is related with the use of multialgebra models. The functions in these models (from values to sets) can be extended point wise to set arguments (from sets to sets) by the additive property of the functions, obtaining a preorder model. It means that the interpretation mapping I has to be defined inductively by additivity. As we will see, to ensure this property we will require the additivity property for all the functions in the signature. This condition is also required by Hussmann [Hus92]. In fact, it becomes his DET-*additive* property by translating $t_2 \in NF^{\supseteq}[f(t_1)]$ into $f(t_1) \longrightarrow t_2 \wedge \text{DET}(t_2)$.

To reduce these four properties to syntactic ones, easier to prove, we need the following lemma.

Lemma 15. *Given a specification* I *containing at least the union axioms, if the orientation and completion of its axioms result in a commutative and terminating bi-rewriting system* $\langle R_{\subseteq}, R_{\supseteq}\rangle$*, then*

1. *If* $NF^{\supseteq} \subseteq NF^{\subseteq}$*, then* $I \vdash_{POL} t_1 \supseteq t_2$ *implies* $NF^{\supseteq}(t_1) \supseteq NF^{\supseteq}(t_2)$.

2. *If* $I \vdash_{POL} t \subseteq \bigcup\{t' \mid t \xrightarrow[R_\supseteq]{} t'\}$ *for any term* $t \notin NF^{\supseteq}$*, then* $NF^{\supseteq}(t_1) \supseteq NF^{\supseteq}(t_2)$ *implies* $I \vdash_{POL} t_1 \supseteq t_2$*.*
3. *If in addition the additive property* $f(\ldots, X \cup Y, \ldots) = f(\ldots, X, \ldots) \cup f(\ldots, Y, \ldots)$ *for any function symbol* $f \in \Sigma$ *holds in the specification* I*, and the bi-rewriting system satisfies* $NF^{\supseteq}[t_1 \cup t_2] = NF^{\supseteq}[t_1] \cup NF^{\supseteq}[t_2]$ *for any pair of terms* t_1 *and* t_2*, then* $t_2 \in NF^{\supseteq}[f(t_1)]$ *implies* $\exists t_3 \in NF^{\supseteq}[t_1] \,.\, t_2 \in NF^{\supseteq}[f(t_3)]$*.*

Proof. 1. Let $I \vdash_{POL} t_1 \supseteq t_2$ hold, the commutation and termination properties of $\langle R_\subseteq, R_\supseteq \rangle$ prove $t_1 \xrightarrow[\supseteq]{*} \circ \xleftarrow[\supseteq]{*} t_2$. Let $t \in NF^{\supseteq}[t_2]$ hold, we have then $t_2 \xrightarrow[\supseteq]{*} t$. The commutation and termination properties prove again $t_1 \xrightarrow[\supseteq]{*} \circ \xleftarrow[\supseteq]{*} t$. However $t \in NF^{\supseteq}$, thus, $t \in NF^{\subseteq}$ by hypothesis, and we have $t_1 \xrightarrow[\supseteq]{*} t$ and therefore $t \in NF^{\supseteq}[t_1]$.
2. The termination property and $I \vdash_{POL} t \subseteq \bigcup\{t' \mid t \xrightarrow{\supseteq} t'\}$ allow to prove by noetherian induction $I \vdash_{POL} t \subseteq \bigcup NF^{\supseteq}[t]$. The union axioms prove $I \vdash_{POL} t \supseteq \bigcup NF^{\supseteq}[t]$ and $I \vdash_{POL} \bigcup NF^{\supseteq}[t_1] \supseteq \bigcup NF^{\supseteq}[t_2]$ if $NF^{\supseteq}[t_1] \supseteq NF^{\supseteq}[t_2]$. Therefore, we have by transitivity $I \vdash_{POL} t_1 \supseteq t_2$.
3. Using the conditions of the previous point we proved $t_1 = \bigcup NF^{\supseteq}[t_1]$; and by the additional conditions of this point we have $f(\bigcup NF^{\supseteq}[t_1]) = \bigcup_{t_3 \in NF^{\supseteq}[t_1]} f(t_3)$ and $NF^{\supseteq}[\bigcup_{t_3 \in NF^{\supseteq}[t_1]} f(t_3)] = \bigcup_{t_3 \in NF^{\supseteq}[t_1]} NF^{\supseteq}[f(t_3)]$. Therefore, if t_2 belongs to this union of sets, then it belongs to one of them, that is, there exists a term $t_3 \in NF^{\supseteq}[t_1]$ such that $t_2 \in NF^{\supseteq}[f(t_3)]$.

Inspired in this SNF-model we can define a new method for checking inclusions. We name this method *nondeterministic computation* method, NDC-method for short, and we define it as follows.

Definition 16. Given a rewriting system $R_\supseteq$ and two terms t and u, the NDC-method is defined by $NDC(t, u) = true$ if, and only if, $NF^{\supseteq}[t] \subseteq NF^{\supseteq}[u]$.

Lemma 17. *If the conditions* $I \vdash_{POL} t \subseteq u$ *and* $NF^{\supseteq}[t] \subseteq NF^{\supseteq}[u]$ *are equivalent, the the NDC-method is sound and complete w.r.t. the class of models* $POAlg(I)$*.*

The following theorem is the main result of this section, and summarizes the results of all the previous lemmas.

Theorem 18. *Given a nondeterministic specification* I*, and a bi-rewriting system* $\langle R_\subseteq, R_\supseteq \rangle$ *resulting from the orientation of its axioms, if the following conditions are satisfied*

1. *the bi-rewriting system is commutative and terminating,*
2. *the axioms defining the union operator can be deduced from* I*,*
3. $NF^{\supseteq} \subseteq NF^{\subseteq}$*,*
4. $I \vdash_{POL} t \subseteq \bigcup\{t' \mid t \xrightarrow{\supseteq} t'\}$ *holds for any term* $t \notin NF^{\supseteq}$*,*
5. $I \vdash_{POL} f(\ldots, X \cup Y, \ldots) = f(\ldots, X, \ldots) \cup f(\ldots, Y, \ldots)$ *for any symbol* $f \in \Sigma$
6. $NF^{\supseteq}[t_1 \cup t_2] = NF^{\supseteq}[t_1] \cup NF^{\supseteq}[t_2]$ *for any terms* t_1 *and* t_2*,*

then the following sentences are equivalent:

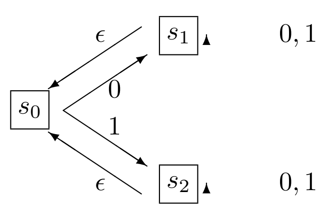
$$\begin{array}{lll} \mathit{POAlg}(I) \models t \subseteq u & I \vdash_{POL} t \subseteq u & t \xrightarrow[R_{\subseteq}]{*} \circ \xleftarrow[R_{\supseteq}]{*} u \\ \overline{\mathit{MAlg}}(I) \models t \subseteq u & & \mathit{NF}^{\supseteq}[t] \subseteq \mathit{NF}^{\supseteq}[u] \end{array}$$

Although these conditions could seem very strange, they hold (or may hold) in most of the nondeterministic specifications. As we will see in the next example, when they do not hold is due to the incompleteness of the specification, the lack of inclusions in $R_{\subseteq}$ without computational meaning, and not to the incompleteness of the rewriting rules $R_{\supseteq}$ used to compute. In these cases it is necessary to add new axioms to the specification, which of course, reduce the number of models, and make the NDC-method and the bi-rewriting method sound and complete.

The same kind of specification completion method has been studied by Hussmann [Hus92].

3.3 An Example of Nondeterministic Specification

To show this specification completion method we will use the classical nondeterministic specification of a nondeterministic automata, in this case an automata to recognize the patterns $(0 \cup 1)^* 0 (0 \cup 1)^*$ and $(0 \cup 1)^* 1 (0 \cup 1)^*$. A first attempt to get a specification is:



$$\begin{array}{ll} X \cup Y \supseteq X & X \cup Y \supseteq Y \\ \mathit{trans}(s_0, 0) \supseteq s_1 & \mathit{trans}(s_0, 1) \supseteq s_2 \\ \mathit{trans}(s_1, X) \supseteq s_1 & \mathit{trans}(s_1, X) \supseteq \mathit{trans}(s_0, X) \\ \mathit{trans}(s_2, X) \supseteq s_2 & \mathit{trans}(s_2, X) \supseteq \mathit{trans}(s_0, X) \\ \mathit{prog}(X, \mathit{nill}) \supseteq X & \\ \multicolumn{2}{l}{\mathit{prog}(X, \mathit{cons}(Y, Z)) \supseteq \mathit{prog}(\mathit{trans}(X, Y), Z)} \end{array}$$

where all inclusions can be oriented to the right, obtaining a commutative bi-rewriting system (where $R_{\subseteq} = \emptyset$). However, it it easy to see that $\mathit{trans}(s_1, X)$ can be reduced by $\xrightarrow{\supseteq}$ to s_1 or to $\mathit{trans}(s_0, X)$, and $I \vdash_{POL} \mathit{trans}(s_1, X) \subseteq s_1 \cup \mathit{trans}(s_0, X)$ does not hold. Therefore the condition $I \vdash_{POL} t \subseteq \bigcup \{t' \mid t \xrightarrow{\supseteq} t'\}$ does not hold for all reducible terms t. This problem can be avoided adding the axiom $\mathit{trans}(s_1, X) \subseteq s_1 \cup \mathit{trans}(s_0, X)$ to the specification. The same happens with $X \cup X$ that can be reduced only to X but $X \cup X \subseteq X$ does not hold; and so on. The additivity condition makes necessary to introduce $\mathit{trans}(X \cup Y, Z) \subseteq \mathit{trans}(X, Z) \cup \mathit{trans}(Y, Z)$ and the same for the second argument and for *prog*.

If we complete the specification in this way we obtain:

$$
\begin{array}{ll}
X \cup Y \supseteq X & X \cup Y \supseteq Y \\
X \supseteq X \cup X & \\
trans(s_0, 0) \supseteq s_1 & trans(s_0, 1) \supseteq s_2 \\
trans(s_1, X) = s_1 \cup trans(s_0, X) & trans(s_2, X) = s_2 \cup trans(s_0, X) \\
prog(X, nill) = X & \\
prog(X, cons(Y, Z)) = prog(trans(X, Y), Z) & \\
trans(X, Z) \cup trans(Y, Z) \supseteq trans(X \cup Y, Z) & \\
trans(Z, X) \cup trans(Z, Y) \supseteq trans(Z, X \cup Y) & \\
prog(X, Z) \cup prog(Y, Z) \supseteq prog(X \cup Y, Z) & \\
prog(Z, X) \cup prog(Z, Y) \supseteq prog(Z, X \cup Y) &
\end{array}
$$

which can be oriented to obtain the bi-rewriting system

$$
R_{\supseteq} = \begin{cases}
X \cup Y \xrightarrow{\supseteq} X \\
X \cup Y \xrightarrow{\supseteq} Y \\
trans(s_0, 0) \xrightarrow{\supseteq} s_1 \\
trans(s_0, 1) \xrightarrow{\supseteq} s_2 \\
trans(s_1, X) \xrightarrow{\supseteq} s_1 \\
trans(s_1, X) \xrightarrow{\supseteq} trans(s_0, X) \\
trans(s_2, X) \xrightarrow{\supseteq} s_2 \\
trans(s_2, X) \xrightarrow{\supseteq} trans(s_0, X) \\
prog(X, nill) \xrightarrow{\supseteq} X \\
prog(X, cons(Y, Z)) \xrightarrow{\supseteq} prog(trans(X, Y), Z)
\end{cases}
\quad
R_{\subseteq} = \begin{cases}
X \cup X \xrightarrow{\subseteq} X \\
trans(X \cup Y, Z) \xrightarrow{\subseteq} trans(X, Z) \cup trans(Y, Z) \\
trans(Z, X \cup Y) \xrightarrow{\subseteq} trans(Z, X) \cup trans(Z, Y) \\
prog(X \cup Y, Z) \xrightarrow{\subseteq} prog(X, Z) \cup prog(Y, Z) \\
prog(Z, X \cup Y) \xrightarrow{\subseteq} prog(Z, X) \cup prog(Z, Y)
\end{cases}
$$

modulo the associative and commutative axioms for the union.

This new bi-rewriting system satisfies all the restrictions of the theorem 18.

The process described in this example, where a specification is completed – leaving the computational rewriting system $\xrightarrow{\supseteq}$ unchanged– corresponds to the selection of a maximally deterministic model described by Hussmann in [Hus92].

4 Conclusions

We have shown that bi-rewriting systems are a natural computational model of inequality specifications. The main results of standard rewriting have been extended to bi-rewriting. However the completion is still an open problem. We have approached the problem by solving the completion of the inequality specification of distributive lattices. The operational semantics of Unified Algebras can be based on this specification. We have also shown the usefulness of bi-rewriting systems to relate the mathematical and the operational semantics of nondeterministic specifications. Finally, we have given the conditions for the soundness and completeness of a normal form computation procedure and the bi-rewriting method, used to automatice the deduction in nondeterministic specifications. We have also given the conditions for the existence and initiality of a model based on sets of normal forms.

References

[DJ90] N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In J. V. Leeuwen, editor, *Handbook of Theoretical Computer Science*. Elsevier Science Publishers, 1990.

[Hes88] W. H. Hesselink. A mathematical approach to nondeterminism in data types. *ACM Trans. Programming Languages and Systems*, 10:87–117, 1988.

[Hue80] G. Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *Journal of the ACM*, 27(4):797–821, 1980.

[Hus91] H. Hussmann. *Nondeterministic Algebraic Specifications*. PhD thesis, Institut für Informatik, Technische Universität München, München, Germany, 1991.

[Hus92] H. Hussmann. Nondeterministic algebraic specifications and nonconfluent term rewriting. *Journal of Logic Programming*, 12:237–255, 1992.

[JK86] J.-P. Jouannaud and H. Kirchner. Completion on a set of rules modulo a set of equations. *SIAM J. computing*, 15(1):1155–1194, 1986.

[Kap86a] S. Kaplan. Rewriting with a nondeterministic choice operator: from algebra to proofs. In *Proc. 1986 European Symp. on Programming*, volume 213 of *Lecture Notes in Computer Science*, pages 351–374. Springer, 1986.

[Kap86b] S. Kaplan. Simplifying conditional term rewriting systems: Unification, termination and confluence. Technical Report 316, Laboratoire de Recherche en Informatique, Universite de Paris-Sud, Orsay, France, 1986.

[Kap88] S. Kaplan. Rewriting with a nondeterministic choice operator. *J. of Theoretical Computer Science*, 56:37–57, 1988.

[LA93] J. Levy and J. Agustí. Bi-rewriting, a term rewriting technique for monotonic order relations. In *RTA'93*, volume 690 of Lecture Notes in Computer Science, pages 17–31, Montreal, Canada, 1993. Springer-Verlag.

[Lev93] J. Levy. Second-order bi-rewriting systems. Technical report, Institut d'Investigació en Intel·ligència Artificial, CSIC, 1993.

[Mes90] J. Meseguer. Rewriting as a unified model of concurrency. In *Concur'90*, Lecture Notes in Computer Science, Amsterdam, The Netherlands, 1990. Springer-Verlag.

[Mes92] J. Meseguer. Conditional rewriting logic as a unified model of concurrency. *J. of Theoretical Computer Science*, 96:73–155, 1992.

[Mos89] P. D. Mosses. Unified algebras and institutions. In *Principles of Programming Languages Conference*, pages 304–312. ACM Press, 1989.

[Nip86] T. Nipkow. Nondeterministic data types: Models and implementations. *Acta Informatica*, 22:629–661, 1986.

[PS81] G. E. Peterson and M. E. Stickel. Complete sets of reductions for some equational theories. *Journal of the ACM*, 28(2):233–264, 1981.