On n-Syntactic Equational Theories*

Alexandre Boudet and Evelyne Contejean

LRI, CNRS URA 410
Université Paris-Sud, Centre d'Orsay
91405 Orsay Cedex

Abstract. We define the n-syntactic theories as a natural extension of the syntactic theories. A n-syntactic theory is an equational theory which admits a finite presentation in which every proof can be performed with at most n applications of an axiom at the root,but no finite presentation in which every proof can be performed with at most $n-1$ applications of an axiom at the root. The n-syntactic theories inherit the good properties of the syntactic theories for solving the word problem, or matching or unification problems. We show that for any integer $n \geq 1$, there exists a n-syntactic theory.

1 Introduction

The solving of symbolic constraints is a major problem for constraint logic programming. Unification constraints, and in particular unification in equational theories, are among the most frequently encountered symbolic constraints. Unification has been widely studied for particular equational theories as well as for arbitrary theories.

Besides general E-unification [6], two major directions, narrowing and syntactic theories have been investigated these last years. This paper extends the notion of syntactic theories to the case where not one, but a bounded number of replacements of equals by equals at the root are necessary to perform any equational proof. We define the n-syntactic theories to which the results for syntactic theories extend naturally (this is easy) and show that n-syntactic theories do really exist (this is more difficult).

Kirchner [7] has defined the syntactic theories as the collapse-free equational theories E which have a *resolvent presentation* A, that is a finite presentation such that two E-equal terms can always be proved equal with at most one application of an axiom of A at the root.

The knowledge that any equality proof needs at most one application of an axiom at the root leads to a dramatic cut of the search space for solving the word problem, or matching or unification problems. It is remarkable that back in '81, Kozen's results on ground equational theories [10] already used the fact that ground theories are syntactic.

* This research was supported in part by GRECO Programmation CNRS and ESPRIT Working Group COMPASS.

Arnborg and Tidén [1] have solved the problem of unification modulo the one-sided distributivity, presented by the axiom $x * (y + z) = (x * y) + (x * z)$. Their algorithm is based on the fact that one-sided distributivity is a syntactic theory, even if the generality of their method was not known at that time. The algorithm uses the three following results:

1. $s_1 * s_2 \stackrel{?}{=} t_1 * t_2$ and $s_1 \stackrel{?}{=} t_1 \ \wedge \ s_2 \stackrel{?}{=} t_2$ have the same solutions.
2. $s_1 + s_2 \stackrel{?}{=} t_1 + t_2$ and $s_1 \stackrel{?}{=} t_1 \ \wedge \ s_2 \stackrel{?}{=} t_2$ have the same solutions.
3. $s_1 * s_2 \stackrel{?}{=} t_1 + t_2$ and $\exists x_1, x_2 : \ s_2 \stackrel{?}{=} x_1 + x_2 \ \wedge \ t_1 \stackrel{?}{=} s_1 * x_1 \ \wedge \ t_2 \stackrel{?}{=} s_1 * x_2$ have the same solutions.

What these results actually prove is that one-sided distributivity is a syntactic theory and the authors used this fact for solving unification problems. The difficult part of their paper is the termination proof. Unfortunately, Arnborg and Tidén's algorithm does not provide any help for the general case, namely the unification problem for any syntactic theory. This is because their termination proof cannot be extended, for it strongly uses some specific properties of the one-sided distributivity. Moreover, Klay [9] has proved that there exists a syntactic theory in which the word problem is undecidable. Hence there are some syntactic theories in which the unification problem is undecidable. Some theories, such as associativity-commutativity, are known to be syntactic and to have a decidable unification problem, but we do not how to use the syntacticness for associative-commutative unification.

At the very beginning, commutativity and permutative theories presented by axioms of the form

$$f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

seemed to be the only syntactic theories, until Kirchner and Klay [8] have shown that a theory E is syntactic if and only if all the equations of the form

$$f(x_1, \ldots, x_n) \stackrel{?}{=} g(y_1, \ldots, y_m)$$

have a finite complete set of most general E-unifiers. In particular, associativity-commutativity (AC) is a syntactic theory, but the usual presentation, consisting of the two axioms

$$(x + y) + z = x + (y + z)$$
$$x + y = y + x$$

is not a resolvent presentation. Figure 1 gives a resolvent presentation of the associative-commutative theory of $+$, borrowed from [8].

Nipkow [11] shows how some rules, derived from a resolvent presentation, may be added to the rules of equality (reflexivity, symmetry, transitivity and functional reflexivity), yielding a PROLOG program for solving matching problems. In addition, Nipkow gives a geometrical interpretation of each equation of the resolvent presentation of AC in term of area covering.

Unfortunately, Klay [9] has proved that

$$x + y = y + x$$

$$(x + y) + z = x + (y + z)$$

$$(x + y) + z = (x + z) + y$$

$$x + (y + z) = y + (x + z)$$

$$(x + y) + (z + t) = (x + z) + (y + t)$$

Fig. 1. Resolvent presentation of the *AC* theory of +

1. Syntacticness is undecidable,
2. there exists a syntactic theory in which the word problem is undecidable.

Kirchner and Klay [8] have shown that the theory of mid-commutativity, presented by the only axiom

$$(x + y) + (z + t) = (x + z) + (y + t)$$

is not syntactic, and they conjectured that every proof needs at most two applications of an axiom at the root. The existence, for $n > 1$ of a *n-syntactic theory*, that is a theory E such that

- E has a finite presentation A in which any proof can be performed with at most n applications of an axiom at the root.
- E has no finite presentation A in which any proof can be performed with at most $n - 1$ applications of an axiom at the root.

was left open until now.

In the following, we show that the n-syntactic theories have the same good properties as the syntactic theories, and we show the existence of a n-syntactic theory for every $n > 1$.

2 Syntactic Theories and n-Syntactic Theories

We assume the reader is familiar with the notions of term algebra, substitution, equational theory, equational and rewrite proof. Our notations are consistent with [5], for instance, we use postfix notation for substitution application; $t|_p$ denotes the subterm of t at position p; $t[u]_p$ is the term obtained by replacing in t the subterm at position p by u. The root position of a term is denoted by Λ and the top function symbol of t is $t(\Lambda)$.

Given a signature $\mathcal{F}$ and a set $\mathcal{X}$ of variables, $\mathcal{T}(\mathcal{F}, \mathcal{X})$ is the free $\mathcal{F}$-algebra over $\mathcal{X}$. An *equational axiom* is an unordered pair $< l, r >$ of terms of $\mathcal{T}(\mathcal{F}, \mathcal{X})$, denoted by $l = r$. Given a set A of equational axioms, we have a *one-step proof* $s \leftrightarrow t$ if there exists an axiom $l = r \in A$, a substitution σ and a position p of s such that $s|_p = l\sigma$ and $t = s[r\sigma]_p$. If $p = \Lambda$, then such a one-step proof is called a *Λ-step*.

The *equational theory* E presented by A is the least congruence containing all the instances of the axioms of A and it coincides with the reflexive-transitive closure $\overset{*}{\leftrightarrow}$ of $\leftrightarrow$. The set A of axioms is called a *presentation* of E. We write $s =_E t$ if there is a proof $s \overset{*}{\leftrightarrow} t$ and we call it an *equational theorem*. An equational theory is *collapse-free* if it has no theorem $x =_E t[x]_p$, with $x \in \mathcal{X}$ (or, equivalently no presentation containing an axiom $x = t[x]_p$) with $p \neq \Lambda$.

Definition 1
A presentation A of an equational theory E is n-resolvent *if A is finite and for every equational theorem $s =_E t$, there exists a proof $s \overset{*}{\leftrightarrow} t$ in which there are at most n Λ-steps.*
A collapse-free equational theory E is syntactic *if it has a 1-resolvent presentation.*
A collapse-free equational theory E is n-syntactic *if it has a n-resolvent presentation but no $n-1$-resolvent presentation*[1].

Comon *et al.* [2] have dropped the assumption that the theories are collapse-free and introduced the notion of *cycle-syntacticness* for solving cyclic equations in the *shallow equational theories*, that is the theories presented by a set of axioms where all the variables are at depth at most one. In the case of n-syntactic theories, it does not make sense to drop the assumption that the theories are collapse-free since every theorem in a collapsing theory has a proof with exactly two Λ-steps: assume $x = t[x]_p$ is an axiom of A and that we have a proof $s \overset{*}{\leftrightarrow} s'$. Then, we have a proof

$$s \leftrightarrow t[s]_p \overset{*}{\leftrightarrow} t[s']_p \leftrightarrow s'$$

where the only Λ-steps are the first one and the last one.

2.1 Properties of the n-Syntactic Theories

The main advantage that we can take of the knowledge that the number of Λ-steps is bounded in a proof using a n-resolvent presentation is the use of efficient complete strategies for solving the word problem, or matching or unification problems.

The contents of this section is a straightforward extension of the previous works on syntactic theories.

[1] According to this definition, Kirchner's syntactic theories are either 0-syntactic (free theory) or 1-syntactic.

Succeed

$s \overset{?}{\underset{i}{\longleftrightarrow}} s \quad \Rightarrow \quad T$

Λ-step

$l\sigma \overset{?}{\underset{i}{\longleftrightarrow}} t \quad \Rightarrow \quad r\sigma \overset{?}{\underset{i-1}{\longleftrightarrow}} t$

if $l = r \in A$ and σ is a substitution and $i \geq 1$

$\neq \Lambda$-step

$s[l\sigma]_p \overset{?}{\underset{i}{\longleftrightarrow}} t \quad \Rightarrow \quad s[r\sigma]_p \overset{?}{\underset{i}{\longleftrightarrow}} t$

if $l = r \in A$ and σ is a substitution and $p \neq \Lambda$

Decompose

$f(s_1, \ldots, s_m) \overset{?}{\underset{0}{\longleftrightarrow}} f(t_1, \ldots, t_m) \quad \Rightarrow \quad s_1 \overset{?}{\underset{n}{\longleftrightarrow}} t_1 \ \wedge \ \cdots \ \wedge \ s_m \overset{?}{\underset{n}{\longleftrightarrow}} t_m$

Decrease

$s \overset{?}{\underset{i}{\longleftrightarrow}} t \quad \Rightarrow \quad s \overset{?}{\underset{i-1}{\longleftrightarrow}} t$

if $i \geq 1$

Clash

$f(s_1, \ldots, s_m) \overset{?}{\underset{0}{\longleftrightarrow}} g(t_1, \ldots, t_k) \quad \Rightarrow \quad F$

if $f \neq g$

Fig. 2. Rules for the word problem in a n-syntactic theory

Word Problem

We introduce the binary predicates $\overset{?}{\underset{i}{\longleftrightarrow}}$ for $0 \leq i \leq n$, and $s\overset{?}{\underset{i}{\longleftrightarrow}}t$ is to be interpreted as "s and t can be proved equal, using the axioms of A, with at most i Λ-steps". Since A is a n-resolvent presentation of E, we have $s =_E t \quad \Leftrightarrow \quad s\overset{?}{\underset{n}{\longleftrightarrow}}t$.

We can solve word problems, that is problems involving the predicates $\overset{?}{\underset{i}{\longleftrightarrow}}$ and the connective $\wedge$, all the variables being implicitely universally quantified.

The set of rules of figure 2 is complete for proving equational theorems. The rules must be applied modulo

- the commutativity of $\overset{?}{\underset{i}{\longleftrightarrow}}$,
- the associativity, commutativity and idempotence of $\wedge$,
- the rewrite rules $\phi \wedge T \to \phi$, $\phi \wedge F \to F$.

Proposition 1

Let E be a n-syntactic equationnal theory and A a n-resolvent presentation of E. Let $s, t \in \mathcal{T}(\mathcal{F}, \mathcal{X})$ such that $s =_E t$. There is a derivation $s\overset{?}{\underset{n}{\longleftrightarrow}}t \quad \Rightarrow \cdots \Rightarrow T$, using the rules of figure 2.

Unification Problems

More interesting is the use of n-syntacticness for unification. For $1 \leq i \leq n$, we introduce the binary predicates $\overset{?}{\underset{i}{=}}$. Given a n syntactic theory E with a n-resolvent presentation A, the solutions of $s\overset{?}{\underset{i}{=}}t$ are the substitutions σ such that there exists a proof $s\sigma \overset{*}{\leftrightarrow} t\sigma$, using the axioms of A, with at most i Λ-steps. Figure 3 gives a complete set of mutation rules for solving unification problems in a n-syntactic theory E which has a n-resolvent presentation A. These rule extend naturally Kirchner's rules for syntactic theories.

Like syntactic theories, n-syntactic theories have a complete set of mutation rules, but if we add a Merge rule or a Replacement rule in order to obtain perform unification, the extended set may not terminate. For example, the mutation and merging process does not terminate for AC theories: there is an infinite derivation starting from the unification problem

$$u + v \overset{?}{=} w + v$$

Indeed, if we perform the mutation using the last equation of figure 1, a merge on v yields a renaming of the original problem.

3 A n-Syntactic Theory for Arbitrary n

Let A_0 be set reduced to the axiom

$$l_0(u_0(x)) = l_1(d_1(x))$$

Mutate

$f(s_1,\ldots,s_m)\overset{?}{\underset{i}{=}}t \quad \Rightarrow \quad r\overset{?}{\underset{i-1}{=}}t \;\wedge\; s_1\overset{?}{\underset{n}{=}}l_1 \;\wedge\; \cdots \;\wedge\; s_m\overset{?}{\underset{n}{=}}l_m$

if $f(l_1,\ldots,l_m) = r \in A$ and $i \geq 1$

Decompose

$f(s_1,\ldots,s_m)\overset{?}{\underset{0}{=}}f(t_1,\ldots,t_m) \quad \Rightarrow \quad s_1\overset{?}{\underset{n}{=}}t_1 \;\wedge\; \cdots \;\wedge\; s_m\overset{?}{\underset{n}{=}}t_m$

Decrease

$s\overset{?}{\underset{i}{=}}t \quad \Rightarrow \quad s\overset{?}{\underset{i-1}{=}}t$

if $i \geq 1$

Clash

$f(s_1,\ldots,s_m)\overset{?}{\underset{0}{=}}g(t_1,\ldots,t_k) \quad \Rightarrow \quad F$

if $f \neq g$

Fig. 3. Mutation rules for unification problems in a n-syntactic theory

and A_i the following set of axioms (for $i \geq 1$)

$$
\begin{aligned}
d_i(a_i(x)) &= b_i(d_i(x)) \\
d_i(r_{i-1}(x)) &= u_i(r_i(x)) \\
b_i(u_i(x)) &= u_i(a_{i+1}(x)) \\
l_i(u_i(x)) &= l_{i+1}(d_{i+1}(x))
\end{aligned}
$$

In the sequel, E_1 is the equational theory presented by A_0 and, for $n \geq 2$, E_n is the theory presented by $A_0 \cup A_1 \cup \cdots \cup A_{n-1}$.

If all the axioms are oriented from left to right, the symbols have the following intuitive meaning:

- l stands for "left" and l_i is the i-th left mark.
- r stands for "right", and r_i is the i-th right mark.
- d_i is a symbol which goes down into a term, changing a_i into b_i until it reaches a right mark.
- u_i is a symbol which goes up into a term, changing b_i into a_{i+1} until it reaches a left mark.

Figure 4 shows a complete search of the class of the term

$$l_0(u_0(a_1(a_1(a_1(r_0(x))))))$$

obtained by applying the axioms of E_3 from left to right.

Proposition 2
For $n \geq 1$, E_n is a n-syntactic equational theory.

The case where $n = 1$ is straightforward, and we assume in the following that $n \geq 2$. The proposition follows from two lemmas. The first lemma shows that E_n has a n-resolvent presentation.

Lemma 1
Let s and t be two E_n-equal terms. Then s and t can be proved equal using the axioms of $A_0 \cup A_1 \cup \cdots \cup A_{n-1}$, with at most n Λ-steps.

Proof:
For $0 \leq i \leq n$ consider the following partial orderings on the alphabet $\mathcal{F} = \{l_0, d_0, a_0, b_0, u_0, r_0\} \cup \cdots \cup \{l_n, d_n, a_n, b_n, u_n, r_n\}$.

- $O_i \ : \ l_i > d_i > b_i > u_i > a_i$
- $\overline{O}_i \ : \ l_i > u_i > b_i > d_i > a_i$

For such a partial ordering P, $Max(P)$ (resp. $Min(P)$) is the maximal (resp. minimal) function symbol for P.
We denote the partial ordering $P \cup P' \cup \{Min(P) > Max(P')\}$ by $P > P'$.
Consider the precedence

$$
\begin{aligned}
&r_n > r_{n-1} > \cdots > r_i > r_0 > r_1 > \cdots > r_{i-1} > O_0 > O_1 > \cdots \\
&\cdots > O_{i-1} > \overline{O}_n > \overline{O}_{n-1} > \cdots > \overline{O}_i
\end{aligned}
$$

$$
\begin{array}{l}
l_0\ (u_0\ (a_1\ (a_1\ (a_1\ (r_0\ (x)))))) \to \\
l_1\ (d_1\ (a_1\ (a_1\ (a_1\ (r_0\ (x)))))) \to \\
l_1\ (b_1\ (d_1\ (a_1\ (a_1\ (r_0\ (x)))))) \to \\
l_1\ (b_1\ (b_1\ (d_1\ (a_1\ (r_0\ (x)))))) \to \\
l_1\ (b_1\ (b_1\ (b_1\ (d_1\ (r_0\ (x)))))) \to \\
l_1\ (b_1\ (b_1\ (b_1\ (u_1\ (r_1\ (x)))))) \to \\
l_1\ (b_1\ (b_1\ (u_1\ (a_2\ (r_1\ (x)))))) \to \\
l_1\ (b_1\ (u_1\ (a_2\ (a_2\ (r_1\ (x)))))) \to \\
l_1\ (u_1\ (a_2\ (a_2\ (a_2\ (r_1\ (x)))))) \to \\
l_2\ (d_2\ (a_2\ (a_2\ (a_2\ (r_1\ (x)))))) \to \\
l_2\ (a_2\ (d_2\ (a_2\ (a_2\ (r_1\ (x)))))) \to \\
l_2\ (a_2\ (a_2\ (d_2\ (a_2\ (r_1\ (x)))))) \to \\
l_2\ (b_2\ (b_2\ (b_2\ (d_2\ (r_1\ (x)))))) \to \\
l_2\ (b_2\ (b_2\ (b_2\ (u_2\ (r_2\ (x)))))) \to \\
l_2\ (b_2\ (b_2\ (u_2\ (a_3\ (r_2\ (x)))))) \to \\
l_2\ (b_2\ (u_2\ (a_3\ (a_3\ (r_2\ (x)))))) \to \\
l_2\ (u_2\ (a_3\ (a_3\ (a_3\ (r_2\ (x)))))) \to \\
l_2\ (u_2\ (a_3\ (a_3\ (a_3\ (r_2\ (x)))))) \to \\
l_3\ (d_3\ (a_3\ (a_3\ (a_3\ (r_2\ (x))))))
\end{array}
$$

Fig. 4. The equivalence class of $l_0(u_0(a_1(a_1(a_1(r_0(x))))))$ for E_3.

Using the recursive path ordering (RPO) [3, 4] extending this precedence, we can prove that the following rewrite system is convergent

$$R^i = R_0 \cup R_1 \cup \cdots \cup R_{i-1} \cup \overline{R_i} \cup \overline{R_{i+1}} \cup \cdots \cup \overline{R_{n-1}}$$

where R_k (resp. $\overline{R_k}$) is the rewrite system obtained by orienting the equations of A_k from left to right (resp. from right to left). Indeed, the RPO orients suitably all the equations, and there are no critical pairs. As an example, the rewrite system R^2 for E_4 and the precedence used to prove its termination are given in figure 5.

$$l_0(u_0(x)) \to l_1(d_1(x))$$

$$\begin{aligned} d_1(a_1(x)) &\to b_1(d_1(x)) \\ d_1(r_0(x)) &\to u_1(r_1(x)) \\ b_1(u_1(x)) &\to u_1(a_2(x)) \\ l_1(u_1(x)) &\to l_2(d_2(x)) \end{aligned}$$

$$\begin{aligned} d_2(a_2(x)) &\leftarrow b_2(d_2(x)) \\ d_2(r_1(x)) &\leftarrow u_2(r_2(x)) \\ b_2(u_2(x)) &\leftarrow u_2(a_3(x)) \\ l_2(u_2(x)) &\leftarrow l_3(d_3(x)) \end{aligned}$$

$$\begin{aligned} d_3(a_3(x)) &\leftarrow b_3(d_3(x)) \\ d_3(r_2(x)) &\leftarrow u_3(r_3(x)) \\ b_3(u_3(x)) &\leftarrow u_3(a_4(x)) \\ l_3(u_3(x)) &\leftarrow l_4(d_4(x)) \end{aligned}$$

Precedence:

$$r_4 > r_3 > r_2 > r_0 > r_1 > l_0 > d_0 > b_0 > u_0 > a_0 > l_1 > d_1 > b_1 > u_1 > a_1$$

$$> l_4 > u_4 > b_4 > d_4 > a_4 > l_3 > u_3 > b_3 > d_3 > a_3 > l_2 > u_2 > b_2 > d_2 > a_2$$

Fig. 5. The rewrite system R^2 for the 4-syntactic theory E_4

Several cases are to be considered:

- The top function symbol of s is l_i for some $i \in \{0, \ldots, n\}$. In this case, t has some l_j for top function symbol, because the axioms can only change l_i into some l_j.

Consider a rewrite proof, using R^i:

$$s \to s_1 \to \cdots s_h \to \cdots \leftarrow t_k \cdots \leftarrow t_1 \leftarrow t$$

Since no rule of R^i can change l_i into some other symbol at the root of a term, no rule applies at the top of s, or any s_h. If $j = i$, the same holds for t and we have a proof with zero Λ-steps. Otherwise, if $j < i$ the only rules of R^i that will apply at the root are

$$l_j(u_j(x)) \to l_{j+1}(u_{j+1}(x)), \ldots, l_{i-1}(u_{i-1}(x)) \to l_i(u_i(x))$$

and we have $i - j$ Λ-steps. Finally, if $j > i$, we have $j - i$ Λ-steps using the axioms

$$l_j(u_j(x)) \to l_{j-1}(u_{j-1}(x)), \ldots, l_{i+1}(u_{i+1}(x)) \to l_i(u_i(x))$$

In every case, the equality proof requires no more than n Λ-steps.

- The top function symbol of s is some a_i or some r_i. In this case, t has the same top function symbol, because no axiom has such a symbol as the top of one of its terms. The proof uses zero Λ-steps.
- The top function symbol of s is some u_i (resp. some d_i). In this case, s is in head normal form for the convergent rewrite system $R^n = R_0 \cup R_1 \cup \cdots \cup R_{n-1}$ (resp. $R^0 = \overline{R_0} \cup \overline{R_1} \cup \cdots \cup \overline{R_{n-1}}$). Now, for s and t to be E_n-equal, the top function symbol of t must be d_i, b_i or u_i, and a rewrite proof will use at most two Λ-steps.
- The top function symbol of s is some b_i. Again, the top function symbol of t must be u_i, b_i or d_i. In the two first cases, R_n will provide a rewrite proof with at most two Λ-steps; in the latter case, such a proof will be obtained with R_0.

In any case, we have shown that there is a convergent rewrite system obtained by orienting suitably the axioms of $A_0 \cup \cdots \cup A_{n-1}$ in which a rewrite E_n-equality proof requires at most n Λ-steps. □

The second lemma shows that E_n has no $n-1$-resolvent presentation.

Lemma 2
Let A be an arbitrary finite presentation of E_n. There exist two E_n-equal terms s and t such that every proof that $s =_E t$ with the axioms of A requires at least n Λ-steps.

Proof:
We assume that A contains all the equational theorems $l =_{E_n} r$ for $| l |=| r |< m$, where m is an arbitrary natural number. Let $s = l_0(u_0(a_1^m(r_0(x))))$. The equivalence class of s for $=_{E_n}$ is

$$\begin{aligned}\overline{s} = \{s\} &\cup \{l_i(b_i^h(d_i(a_i^k(r_{i-1}(x))))) \mid 1 \le i \le n-1, h+k=m\} \\ &\cup \{l_i(b_i^h(u_i(a_{i+1}^k(r_i(x))))) \mid 1 \le i \le n-1, h+k=m\} \\ &\cup \{l_n(d_n(a_n^m(r_{n-1}(x))))\}\end{aligned}$$

A Λ-step $t_1 \leftrightarrow t_2$ with $t_1, t_2 \in \overline{s}$ must use an axiom $l[x]_p = r[x]_p$ of A with $p = \underbrace{1\,1 \cdots 1}_{b<m\ times}$ and $t_1[x]_p = l[x]_p$ and $t_2[x]_p = r[x]_p$. The only pairs $< t_1, t_2 >$ of terms of $\overline{s}$ such that

1. $t_1(\Lambda) \neq t_2(\Lambda)$
2. $t_1[x]_p =_{E_n} t_2[x]_p$ for some position $p = \underbrace{1\,1 \cdots 1}_{b<m\ times}$

are of the form

$$l_i(b_i^h(u_i(a_{i+1}^k(t')))) = l_{i+1}(b_{i+1}^{h'}(d_{i+1}(a_{i+1}^{k'}(t'))))$$

where $h + k = h' + k'$. Hence, if a Λ-step changes the top function symbol of a term in $\overline{s}$ it must use an axiom of A of the form

$$l_i(b_i^h(u_i(a_{i+1}^k(x)))) = l_{i+1}(b_{i+1}^{h'}(d_{i+1}(a_{i+1}^{k'}(x))))$$

Indeed, the only way to change the top symbol l_i of a term is to find either a symbol u_i or a right mark r_{i-1} in the rest of the term. In the terms of $\overline{s}$, the right marks are too deep in the terms for making it possible to use some axioms which are not of the above form.

Hence, every proof, using the axioms of A, that

$$l_0(u_0(a_1^m(r_0(x)))) =_{E_n} l_n(d_n(a_n^m(r_{n-1}(x))))$$

requires n Λ-steps using axioms of the form $l_i(\cdots) = l_{i+1}(\cdots)$. $\square$

More n-Syntactic Theories

The theories E_n were designed in order to have a simple proof of the existence of n-syntactic theories, but there are some more natural non-monadic n-syntactic equational theories. We now give such an example: here is a presentation A of a 3-syntactic theory:

$$(x + y) + z = x + (y + z)$$
$$a + b = b + a$$

The $+$ symbol is associative, and AC on the terms of $\mathcal{T}(\{+, a, b\})$. For any finite presentation A of this theory, there exists an n such that a proof that

$$\underbrace{(a + (\ldots + a)\ldots)}_{n\ times} + \underbrace{(b + (\ldots + b)\ldots)}_{n\ times} \overset{*}{\leftrightarrow} \underbrace{(b + (\ldots + b)\ldots)}_{n\ times} + \underbrace{(a + (\ldots + a)\ldots)}_{n\ times}$$

using the axioms of A requires at least 3 Λ-steps. In addition, the above presentation is 3-resolvent.

An ω-Syntactic Theory

Whether the theories of mid-commutativity and two-sided distributivity are n-syntactic for some n is an open problem. Some theories have no n-resolvent presentation for any n, we call them *ω-syntactic* theories. An simple example of an ω-syntactic theory is the theory E_ω presented by the following axioms:

$$x * (y * z) = (x * y) * z$$
$$x * y = y * x$$
$$(x * a) + (b * y) = (x * b) + (a * y)$$

This can easily be proved by showing that applying a theorem of E_ω to a term of the form $(s * t) + (s' * t')$ can only exchange finitely many occurrences of a on one side of the root with the same number of occurrences of b on the other side. Hence, for any finite presentation of E_ω, a proof that

$$\underbrace{(a * (\cdots * a) \cdots)}_{m\ times} + \underbrace{(b * (\cdots * b) \cdots)}_{m\ times} \overset{*}{\leftrightarrow} \underbrace{(b * (\cdots * b) \cdots)}_{m\ times} + \underbrace{(a * (\cdots * a) \cdots)}_{m\ times}$$

may require arbitrarily many Λ-steps for a large enough m.

4 Conclusion

Syntactic theories have raised more and more interest since Kirchner and Klay [8] have shown that there are many syntactic theories, including all the finitary unifying theories. We have shown that some non-syntactic theories, namely the n-syntactic theories have similar properties that can be used for solving symbolic constraints.

Some criteria are given in [8, 11], which are sufficient conditions for a presentation to be resolvent. The techniques are based on one-step proofs permutations in the proofs that use more than one Λ-step. Similar techniques should apply to define criteria for n-resolvent presentations.

We believe that for solving unification problems, the interesting distinction is not between syntactic and non-syntactic theories but rather between the theories that are n-syntactic for some finite n and ω-syntactic theories. Indeed, unification is undecidable in general in syntactic theories as well as in n-syntactic theories while in both cases, the top-down strategy with at most one (or n) paramodulations at the root is complete. At the moment, we have no idea of any characterization of the ω-syntactic theories.

References

1. S. Arnborg and E. Tidén. Unification problems with one-sided distributivity. In *Proc. Rewriting Techniques and Applications 85, Dijon, LNCS 202*. Springer-Verlag, May 1985.

2. H. Comon, M. Haberstrau, and J.-P. Jouannaud. Decidable properties of shallow equational theories. In *Proc. 7th IEEE Symp. Logic in Computer Science*, Santa Cruz, 1992. Also Research Report, Dec. 1991, Laboratoire de Recherche en Informatique, Orsay, France.
3. Nachum Dershowitz. Orderings for term-rewriting systems. *Theoretical Computer Science*, 17(3):279–301, March 1982.
4. Nachum Dershowitz. Termination of rewriting. *J. Symbolic Computation*, 3(1):69–115, February 1987.
5. Nachum Dershowitz and Jean-Pierre Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, pages 243–309. North-Holland, 1990.
6. J. Gallier and W. Snyder. Complete sets of transformations for general E-unification. *Theoretical Computer Science*, 67:203–260, 1989.
7. C. Kirchner. Computing unification algorithms. In *Proc. 1st IEEE Symp. Logic in Computer Science, Cambridge, Mass.*, pages 206–216, 1986.
8. C. Kirchner and F. Klay. Syntactic theories and unification. In *Proc. 5th IEEE Symp. Logic in Computer Science, Philadelphia*, June 1990.
9. F. Klay. Undecidable properties of syntactic theories. In *Proc. 4th Rewriting Techniques and Applications 91, Como, LNCS 488*, 1991.
10. D. Kozen. Positive first order logic is NP-complete. *IBM Journal of Res. Developp.*, 25(4):327–332, July 1981.
11. T. Nipkow. Proof transformations for equational theories. In *Proc. 5th IEEE Symp. Logic in Computer Science, Philadelphia*, June 1990.