Transforming Infinite Rewrite Systems into Finite Rewrite Systems by Embedding Techniques

Jürgen Avenhaus

SEKI Report SR-89-21

Transforming infinite rewrite systems into finite rewrite systems by embedding techniques

J. Avenhaus

Department of Computer Science
University of Kaiserslautern
6750 Kaiserslautern
West Germany

e-mail: avenhaus@uklirb.uucp

Abstract

The Knuth-Bendix completion procedure can be used to transform an equational system into a convergent rewrite system. This allows to prove equational and inductive theorems. The main draw back of this technique is that in many cases the completion diverges and so produces an infinite rewrite system. We discuss a method to embed the given specification into a bigger one such that the extended specification allows a finite "parameterized" description of an infinite rewrite system of the base specification. Examples show that in many cases the Knuth-Bendix completion in the extended specification stops with a finite rewrite system though it diverges in the base specification. This indeed allows to prove equational and inductive theorems in the base specification.

1. Introduction

Term rewriting systems constitute an important tool to compute and reason in systems defined by equations. Given a set E of equations, the validity problem for E is to decide for any two given terms s, t whether or not the equation s = t follows from the equations in E. We write $s =_E t$ in this case and call s = t an equational theorem of E. The rewrite approach to decide this problem is to transform E by the Knuth-Bendix completion procedure into a convergent rewriting system R such that $=_E \; = \; =_R$. Then R defines for every term t a unique normal form $t{\downarrow}$ and we have $s =_E t$ iff $s{\downarrow} \equiv t{\downarrow}$. The major draw back of this approach is that no finite convergent term rewriting system R for E may exist. So the "preprocessing" of E into R will not stop.

Another application is to prove inductive theorems. It is well-known that $s =_E t$ iff s = t holds in all models of E. For abstract data types one is usually interested in the initial model $\mathfrak{I}(E)$ of E. We have s = t in $\mathfrak{I}(E)$ iff $s\sigma =_E t\sigma$ for every ground substitution σ. We call s = t an inductive theorem in this case. Given a convergent rewriting system R for E one can try to compute R_0 for $E \cup \{s = t\}$. Then s = t is an inductive theorem iff for every rule $l \rightarrow r$ in R_0 the term l is inductively reducible by R [JKo]. Again, if R_0 is infinite then this approach fails.

There are various proposals of how to circumvent divergence of the Knuth-Bendix completion procedure, see [Her] for suggestions. But in general, divergence is one of the most important problems when using rewriting and completion techiques. In [Kir] it is proposed to describe an infinite set of rewrite rules by a finite set of meta rules containing parameters to describe the infinite set of rules. The problem is how to deal with such a parameterized system, e.g. how to test confluence. In [Kir] a rather complicated framework using order-sorted rewriting is developed. Under some strong restrictions completion of parameterized rewrite systems seems possible.

In this paper we discuss a rather simple approach to deal with structures defined by infinite rewrite systems. It is well known that structures allowing only complicated systems of defining equations may be embedded into structures with a rather simple defining equational system. As a consequence, problems in the base structure can be shifted into the extended structure and so may become easier to solve. In general one has to know algebraic properties of the base structure to find an appropriate extension. But when dealing with the completion process in many cases an infinite set of rules (i.e. directed equations) is generated that has some regularities and allows finite descriptions with natural numbers as parameters. So it seems reasonable to extend the base structure one is interested in by a copy NAT of natural numbers. In the extended structure the "parameters" are ordinary variables, so the well developed rewriting techniques can be used to reason in the extended structure and hence in the base structure, too, see [TJa].

In this paper we study what is needed to make this approach work. We point out the problems and give sufficient conditions under which one can overcome these problems. The research was motivated by - but is not restricted to - the extension of a structure by a copy of NAT to get a finite convergent rewriting system as set of defining equations. We will not study the problem how to get the extension automatically from the completion process. There are some proposals to learn by inductive inference generalizations of sequences of terms and this can be used to find an extension of the base structure in which all defining equations of the base structure are valid, see [TJa], [Lan]. In [BKR] general-state-machines are used to describe infinite rewrite systems produced by the completion procedure for string rewriting.

We assume the reader to be familiar with rewriting and completion techniques as developed in [KBe] and [Hue]. For a survey see [AMa]. We use the standard notations as in [Hue]. If R is a rewrite system then $\Longrightarrow_R$ denotes the rewrite relation induced by R. We call R convergent if $\Longrightarrow_R$ is confluent and well-founded. We will need rewriting modulo a congruence defined by a set A of equations and denote by $\Longrightarrow_{R/A}$ the relation $=_A \circ \Longrightarrow_R \circ =_A$. We say R/A is a convergent rewrite system for the equational system E (or R is convergent modulo A) iff (i) R/A is terminating, i.e. there is no infinite sequence $t_0 \Longrightarrow_{R/A} t_1 \Longrightarrow_{R/A} \ldots$ and (ii) R/A is Church-Rosser modulo A, i.e. $s =_{R \cup A} t$ implies $\hat{s} =_A \hat{t}$ for some terms $\hat{s}, \hat{t}$ with $s \overset{*}{\Longrightarrow}_{R/A} \hat{s}$ and $t \overset{*}{\Longrightarrow}_{R/A} \hat{t}$ and (iii) E is equivalent to $R \cup A$, i.e. $s =_E t$ iff $s =_{R \cup A} t$. For completion procedures that try to transform E into R,A see [PSt], [JKi], [BDe]. Here one can also find other rewriting relations $\Longrightarrow_0$ with $\Longrightarrow_R \subseteq \Longrightarrow_0 \subseteq \Longrightarrow_{R/A}$ for condition (ii) which have some practical advantages.

We denote by $\equiv$ the identity of terms, by Th(E) the set of equational theorems and by ITh(E) the set of inductive theorems of E. The paper is organized as follows. We start in section 2 with a motivating example. In sections 3 and 4 the embedding strategy is presented and applications to prove equational and inductive theorems are discussed. In section 5 we show how to test the conditions which are necessary for the approach to work and give in section 6 some examples to show the power of the method.

2. An example

As a motivating example for our approach let us consider the specification NAT of the natural numbers with the gcd-function, see e.g. [Her].

$$
\begin{array}{llll}
E: & x+0 = x & g(x,0) = x & g(x+y,y) = g(x,y) \\
 & x+s(y) = s(x+y) & g(0,y) = y & g(x,y+x) = g(x,y)
\end{array}
$$

One may transform this equational system into a rewrite system R_0 by orienting the equations from left to right. Unfortunately R_0 is not confluent, so it cannot be used to compute the gcd of two numbers i and j. Notice that $g(s^i(o), s^j(o))$ is irreducible in R_0. We would like to have a convergent rewrite system R for E, this would allow to compute $g(s^i(o), s^j(o))$ and to prove equational theorems of E. Furthermore, we would like to prove inductive theorems of E, e.g. $g(x,x) = x$.

Completion of E using the ordering RPO (see [Der]) with precedence $+ > s$ results in four infinite sequences of rules

$$
\begin{array}{lcl}
g(s^n(x), s^n(o)) & \rightarrow & g(x,s^n(o)) \\
g(s^n(o), s^n(y)) & \rightarrow & g(s^n(o),y) \\
g(s^n(x+y), s^n(y)) & \rightarrow & g(x,s^n(y)) \\
g(s^n(x), s^n(y+x)) & \rightarrow & g(s^n(x),y)
\end{array}
$$

It is natural to look for an embedding that contains a copy of the natural numbers and to express $s^n(x)$ by $S(n,x)$ where S is a new function symbol. To do so we specify the copy of natural numbers by the operators $\underline{1}$ and $\underline{+}$ and the equations

$$
\text{(AC)} \quad u \,\underline{+}\, v = v \,\underline{+}\, u \qquad\qquad (u\underline{+}v) \,\underline{+}\, w = u \,\underline{+}\, (v\underline{+}w)
$$

Now we define the new operator S by

$$
\begin{array}{ll}
\text{(S)} & s(x) = S(\underline{1},x) \\
 & S(u,S(v,x)) = S(u\underline{+}v,x)
\end{array}
$$

If we start the completion procedure with E_2 consisting of E and (S) and (AC) then the completion process again diverges. But from the set of rules being produced one can see that the following equation is missing.

$$
\text{(S1)} \quad x+S(u,y) = S(u,x+y)
$$

Note that this equation generalizes $x+s(y) = s(x+y)$ to $x+s^n(y) = s^n(x+y)$ which for every $n \in \mathbb{N}$ is an equational theorem of E and so is valid. If we add the equation (S1) then the completion procedure stops successfully with

$$
\begin{array}{lll}
R: & x+0 & \to x \\
 & x+S[u,y] & \to S[u,x+y] \\
 & g[x,0] & \to x \\
 & g[0,y] & \to y \\
 & g[S[u,x+y],\ S[u,y]] & \to g[x,S[u,y]] \\
 & g[S[u,x],\ S[u,0]] & \to g[x,S[u,0]] \\
 & g[S[u,x],\ S[u,y+x]] & \to g[S[u,x],y] \\
 & g[S[u,0]],\ S[u,y]] & \to g[S[u,0],y] \\
 & g[S[u \underline{+} v,x],\ S[u,0]] & \to g[S[v,x],\ S[v,0]] \\
 & g[S[u,0]],\ S[u \underline{+} v,x]] & \to g[S[u,0],\ S[v,x]] \\
 & \underline{+} \text{ is AC} &
\end{array}
$$

$$
\begin{array}{ll}
s[x] & \to S[\underline{1},x] \\
S[u,S[v,x]] & \to S[u \underline{+} v,x] \\
g[x+y,y] & \to g[x,y] \\
g[x,y+x] & \to g[x,y]
\end{array}
$$

Using this finite rewrite system R we can prove the inductive theorem $g[x,x] = x$ of E by the method "proof by consistency", see [JKo]: We complete $R \cup \{g[x,x] = x\}$ and get as result the system R and the rule $g[x,x] \to x$. Since $g[x,x]$ is inductively reducible by R we have proved that $g[x,x] = x$ is indeed an inductive theorem of E.

We are going to make these ideas precise in the rest of the paper.

3. The embedding strategy

Assume we have two specifications $spec_1$ and $spec_2$ such that $spec_1$ is a subspecification of $spec_2$ (for definitions see below). In this section we study how to use $spec_2$ to compute and prove equational theorems in $spec_1$. This will need a careful definition of what it means that $spec_2$ is a consistent enrichment of $spec_1$. Note that by the theorem of Birkhoff s = t is an equational theorem of $spec_1$ iff s = t holds in all models of $spec_1$. We will use equational reasoning in $spec_2$ but do not consider all models of $spec_2$. This allows to add "valid equations", and in many applications these additional valid equations help to get a finite convergent rewrite system in $spec_2$ to reason in the given base specification $spec_1$.

A <u>specification</u> spec = $(\Sigma,F;E)$ consists of a signature sig = (Σ,F) and a set E of defining equations. Here Σ is a set of sorts and F is a set of operators, each operator f with a fixed arity $\tau(f)$: $s_1,\ldots,s_n \rightarrow s$ where s_i, $s \in \Sigma$. For each sort s we assume to have a denumerable set V_s of variables such that $V_s \cap V_{s'} = \emptyset$ for $s \neq s'$. Then V is the union of all V_s and Term(F,V) is the set of terms over the set F of operators and the set V of variables.

If $spec_1 = (\Sigma_1,F_1;E_1)$ and $spec_2 = (\Sigma_2,F_2;E_2) = (\Sigma_1 \cup \Sigma_0,\ F_1 \cup F_0;\ E_1 \cup E_0)$ then $spec_1$ is a <u>subspecification</u> of $spec_2$. Let V_1 be the set of variables of sorts $s \in \Sigma_1$ and V_0 the set of variables of sorts $s \in \Sigma_0$. Then the elements of V_0 are called <u>parameters</u>. An order-preserving substitution ψ: $V_0 \rightarrow Term(F_0,\emptyset)$ is called a <u>parameter substitution</u>. A term $t \in Term(F_1 \cup F_0,\ V_1)$ in the extended specification $spec_2$ is <u>reachable</u> if there is a term $t' \in Term(F_1,V_1)$ in the base specification $spec_1$ such that $t' =_{E2} t$. We say t is reachable from t' in this case.

We call $spec_2$ a <u>consistent enrichment</u> of $spec_1$ if the following holds:

> If $t_1 = t_2$ is in E_0, ψ is a parameter substitution and $\psi(t_i)$ is reachable from t_i' for i = 1,2, then $t_1' =_{E1} t_2'$.

In other words, $spec_2$ is a consistent enrichment of $spec_1$ if the equations in E_0 do not introduce new equalities among the terms in the base specification $spec_1$.

In our gcd-example of the previous section we have $spec_1$ = ({NAT}, {0,s,+,g}; E_1) with E_1 consisting of the six equations in E. To get $spec_2$ we add the sort NAT_+ and the operators in F_0 = {<u>1</u>,<u>+</u>,S} with $\tau(S)$ = NAT_+, NAT $\rightarrow$ NAT. (Notice that we are dealing with many sorted signatures so that NAT and NAT_+ are completely different sorts). Finally, we add the set E of defining equations consisting of the equations (AC) and (S). It is easy to see that (1) every term $t \in Term(F_1 \cup F_0,\ V_1)$ is reachable and (2) $spec_2$ is a consistent enrichment of $spec_1$. For (2) see section 5.

If a term t $\in$ Term$(F_1 \cup F_0, V_1 \cup V_0)$ contains parameters $x \in V_0$, then t describes all the terms $\psi(t) \in$ Term$(F_1 \cup F_0, V_1)$ with ψ a parameter substitution. So an equation $t_1 = t_2$ describes all the equations $\psi(t_1) = \psi(t_2)$. This allows in many situation the finite description of an infinite set of $spec_1$-equations in $spec_2$.
To make this precise we define an equation $t_1 = t_2$ with $t_1, t_2 \in$ Term$(F_1 \cup F_0, V_1 \cup V_0)$ to be <u>valid</u> with respect to $spec_2$ and $spec_1$ if $\psi(t_1) =_{E2} \psi(t_2)$ for each parameter substitution ψ such that $\psi(t_1)$ or $\psi(t_2)$ is reachable. This gives immediately

Fact 3.1: If $spec_2$ is a consistent enrichment of $spec_1$ and each equation in E is valid with respect to $spec_2$ and $spec_1$, then $spec_3 = (\Sigma_2, F_2; E_2 \cup E)$ is a consistent enrichment of $spec_1$. ∎

Coming back to our gcd-example, we have $x + s^n(y) =_E s^n(x+y)$ for all $n \geq 1$, so

$$x + S(u,y) = S(u,x+y)$$

is valid with respect to $spec_2$ and $spec_1$.

Now assume $spec_2$ is a consistent enrichment of $spec_1$. We may run the completion procedure with input E_2 and an appropriate reduction ordering, thereby regarding both the "variables" in $spec_1$ and the "parameters" in $spec_2$ as variables. Then new equations are produced by equational reasoning. These equations are automatically valid, so all specifications produced by the completion procedure are consistent enrichments by Fact 3.1. In many cases one needs rewriting and completion modulo a set A of unorientable equations. This gives

Fact 3.2: Assume $spec_2 = (\Sigma_2, F_2; E_2)$ is a consistent enrichment of $spec_1$ and E is a set of equations that are valid with respect to $spec_2$ and $spec_1$. If completion of $E_2 \cup E$ results in $R \cup A$ such that R is convergent modulo A then $spec_3 = (\Sigma_2, F_2; R \cup A)$ is a consistent enrichment of $spec_1$. ∎

Now suppose our approach was successful, i.e. we have found for $spec_1$ a consistent enrichment $spec_2$ with a finite convergent rewrite system as set of defining equations. Then we can decide E_1-equality by the next theorem

Theorem 3.3:

If $spec_2 = (\Sigma_2, F_2; R \cup A)$ is a consistent enrichment of $spec_1 = (\Sigma_1, F_1; E_1)$ and R is convergent modulo A then $s =_{E1} t$ iff $\hat{s} =_A \hat{t}$ where $\hat{s}$ and $\hat{t}$ denote R/A-normal forms of s and t. ∎

4. Proving inductive theorems

The method described in section 3 can easily be modified to prove inductive theorems. To do so we use the approach of Jouannaud and Kounalis [JKo]: If R is a rewrite system for E and R_0 is a convergent rewrite system for $R \cup E_0$ such that $R \subseteq R_0$ and every left-hand side l of a rule $l \rightarrow r$ in R_0 is inductively reducible by R then $E_0 \subseteq ITh(E)$. Here the condition $R \subseteq R_0$ can be dropped, then R needs only be terminating, it will automatically be ground-confluent.

Theorem 4.1:

Assume $spec_1 = (\Sigma_1, F_1; E_1)$ is given and $spec_2 = (\Sigma_1 \cup \Sigma_0, F_1 \cup F_0; R_2 \cup A)$ is a consistent enrichment of $spec_1$ such that R_2/A is terminating. Assume also that E is a set of equations in $spec_1$. If R/A is a convergent rewrite system for $R_2 \cup A \cup E$ such that for each rule $l \rightarrow r$ in R the term l is inductively reducible by R_2/A, then $R \cup A \subseteq ITh(R_2 \cup A)$ and $E \subseteq ITh(E_1)$.

Proof: a) To prove $R \cup A \subseteq ITh(R_2 \cup A)$ we have to show $t_1 =_{R_2 \cup A} t_2$ whenever $t_1 =_{R \cup A} t_2$ and t_1, t_2 are ground terms. If $t_1 =_{R \cup A} t_2$ then t_1 and t_2 have a common R/A-normal form t. Let $t_i \overset{*}{\Longrightarrow}_{R_2/A} \hat{t}_i$ such that $\hat{t}_i$ is R_2/A-irreducible, i = 1,2. Then $\hat{t}_i =_{R \cup A} t$ and $\hat{t}_i \overset{*}{\Longrightarrow}_{R/A} t_i' =_A t$ for some t_i', since R/A is confluent modulo A and t is R/A irreducible. If $\hat{t}_i$ is different from t_i' then $\hat{t}_i$ is reducible by some rule $l \rightarrow r$ in R. Since l is inductively reducible by R_2/A this implies that $\hat{t}_i$ is reducible by R_2/A. But $\hat{t}_i$ was a R_2/A-normal form and so irreducible in R_2/A. This gives $\hat{t}_1 =_A t =_A \hat{t}_2$ and so $t_1 =_{R_2 \cup A} t_2$.
b) To prove $E \subseteq ITh(E_1)$ we have to show $\sigma(s) =_{E_1} \sigma(t)$ for every equation s = t in E and every ground substitution σ. We have $\sigma(s) =_{R \cup A} \sigma(t)$ since R is a rewrite system modulo A for $R_2 \cup A \cup E$. This and a) give $\sigma(s) =_{R_2 \cup A} \sigma(t)$ and since $spec_2$ is a consistent enrichment of $spec_1$ we have $\sigma(s) =_{E_1} \sigma(t)$. ∎

Let us look at an example to show how Theorem 2 is used. Assume

E_1: $0 + y = y$
$s(x) + y = x + s(y)$

and we want to prove that $x + 0 = x$ is an inductive theorem of E_1. The completion procedure with input E and the equation $x + 0 = x$ diverges and generates the rules $x + s^n(0) \rightarrow s^n(x)$. So we use as extension the rules

$s(x) \rightarrow S(\underline{1}, x)$
$S(u, S(v, x)) \rightarrow S(u \underline{+} v, x)$
$\underline{+}$ is AC

The completion with E_1 and these equations as input produces the convergent rewrite system modulo (AC)

$$
\begin{array}{llll}
R_2: & 0 + y \rightarrow y & & S(\underline{1},x) + y \rightarrow x + S(1,y) \\
 & s(x) \rightarrow S(\underline{1},x) & & S(\underline{1+}u,\, x) + y \rightarrow S(u,x) + S(\underline{1},y) \\
 & \underline{+} \text{ is AC} & & S(u,S(v,x)) \rightarrow S(u\underline{+}v,\, x)
\end{array}
$$

Now adding $x + 0 = x$ to R_2 and starting the completion procedure again produce the rules

$$x + S(\underline{1} \,\underline{+}\, \dots \,\underline{+}\, \underline{1},\ 0) \rightarrow S(\underline{1} \,\underline{+}\, \dots \,\underline{+}\, 1,\ x)$$

So we add as inductive hypothesis the equation

$$x + S(u,0) \rightarrow S(u,x)$$

and the completion procedure produces

$$
\begin{array}{lll}
R : R_2 \text{ and} & x + 0 & \rightarrow x \\
 & x + S(u,0) & \rightarrow S(u,x)
\end{array}
$$

Since both left-hand sides $x + 0$ and $x + S(u,0)$ are inductively reducible by R/AC we have proved $x + 0 = x$ is in ITh(E).

5. Proving "consistent enrichment"

In this section we study how to deal with the conditions that are necessary for the embedding strategy to work.

The first problem is how to prove that $spec_2$ is a consistent enrichment of $spec_1$. This problem is in general undecidable, but there are sufficient conditions for this property. Let $E_2 = E_1 \cup E_0$ where E_0 is

E_0: $S(\underline{1},x) = s(x)$ $\qquad$ $S(u,S(v,x)) = S(u\underline{+}v,x)$
$\underline{+}$ is AC

Notice that we have oriented the first equation from right to left to get a finite convergent rewrite system for E_2. To prove that $spec_2$ is a consistent enrichment of $spec_1$ it is tempting to use the method of Jouannaud and Kounalis [JKo]. This would require to orient the first equation from left to right. But now the completion process for $E_2 = E_0 \cup E_1$ will diverge in our applications and so the method of [JKo] will not work.

We will use the S-equations of E_0 alone, orient then from left to right, run the completion procedure modulo [AC] to get a "parameter-ground confluent" rewrite system R for E_0 and so prove that $spec_2$ is a consistent enrichment of $spec_1$ without changing E_1.

To do so we use the approach of [BDP] for unfailing completion. A reduction ordering is a ground reduction ordering that can be extended to a reduction ordering which is total an ground terms. Many of the standard orderings are indeed ground reduction orderings. An ordering > is A-compatible if $s > t$, $s =_A s'$ and $t =_A t'$ imply $s' > t'$.

The next result gives sufficient conditions to guarantee that $spec_2$ is a consistent enrichment of $spec_1$. These conditions do not depend on $spec_1$. This leads to "uniform consistent extensions".

Theorem 5.1:
Let $spec_1 = (\Sigma_1,F_1;E_1)$, and $spec_2 = (\Sigma_2,F_2; R \cup A \cup E_1)$ be given with $\Sigma_2 = \Sigma_1 \cup \Sigma_0$, $F_2 = F_1 \cup F_0$. Assume
(1) There is an A-compatible ground reduction ordering > with $l > r$ for all $l \to r$ in R.
(2) R is confluent modulo A on the parameter-free $spec_2$-terms.
(3) If $l \to r$ is in R and $u = v$ is in A then l, u and v are F_1-free and not variables.

Then $spec_2$ is a consistent extension of $spec_1$.

Proof: Let $E_2 = R \cup A \cup E_1$ and assume t_1 and t_2 are $spec_1$-terms with $t_1 =_{E_2} t_2$. We have to prove $t_1 =_{E_1} t_2$. Let $\bar{t}_i$ denote the term resulting from t_i by replacing the variables x_j by new constants c_j. We have $t_1 =_{E_i} t_2$ iff $\bar{t}_1 =_{E_i} \bar{t}_2$ for i = 1,2.

It is easy to see that > is also a ground reduction ordering on the signature $sig_2^!$ resulting from $sig_2 = (\Sigma_2, F_2)$ by adding the new constants c_j. So we may run the unfailing Knuth-Bendix completion procedure of [BDP] with input E_1 and reduction ordering >. Let (E^∞, R^∞) be the result and let $\bar{R} = R^\infty \cup R_\infty$ where R_∞ is the set of orientable $sig_2^!$-instances of equations in E^∞. Then $\bar{R}$ is ground confluent on the ground $sig_1^!$-terms. Since by condition (3) there are no critical pairs between $\bar{R}$ and R or between $\bar{R}$ and A, the system $R \cup \bar{R}$ is ground confluent modulo A on the $sig_2^!$-terms. Since $\bar{t}_1 =_{E_2} \bar{t}_2$ this implies the existence of some term $\bar{t}$ with $\bar{t}_1 \overset{*}{\Longrightarrow} \bar{t} \overset{*}{\Longleftarrow} \bar{t}_2$ where $\Longrightarrow$ is $\Longrightarrow_{(R \cup \bar{R})/A}$. Since $\bar{t}_i$ are F_1-free there is, by condition (3), no R-rule or A-equation used in this derivation. This shows $\bar{t}_1 \overset{*}{\Longrightarrow}_{\bar{R}} \bar{t}\ {}_{\bar{R}}\overset{*}{\Longleftarrow} \bar{t}_2$, so $\bar{t}_1 =_{E_1} \bar{t}_2$ and so $t_1 =_{E_1} t_2$. ∎

Given $spec_1$ and $spec_2$ with $E_2 = E_1 \cup E_0$, we do not address in detail the problem how to transform E_0 into $R \cup A$ such that R is confluent modulo A on the parameter-free terms. The simplest way is to run the completion procedure modulo A with input E. This may result in a rewrite system R such that not every left-hand side of a rule is F_1-free. Here techniques to find a ground confluent system may help (see [Fri], [Göb], [Kue]).

To see how Theorem 5.1 is applied assume we have $spec_2 = \langle \Sigma_1 \cup \Sigma_0, F_1 \cup F_0, E_1 \cup E_0 \rangle$ with $F_0 = \{S, \underline{1}, \underline{+}\}$ and

E_0: $S(\underline{1},x) = s(x)$
$S(u,S(u,v)) = S(u \underline{+} v,x))$
$u \underline{+} v = v \underline{+} u$ $\qquad (u \underline{+} v) \underline{+} w = u \underline{+} (v \underline{+} w)$

as above. We use the polynomial ordering [Der] with interpretation Θ of the operators

$\Theta(S)\ (n,m) = (n + m)^2$ $\qquad \Theta(\underline{1}) = 1$
$\Theta(\underline{+})\ (n,m) = n + m$
$\Theta(f)\ (n_1,\dots,n_k) = n_1 + n_2 + \dots + n_k + 1$ $\qquad$ for all $f \in F_1$

Running the completion procedure modulo (AC) with input E_0 gives the rewrite system

R' (1) $S(1,x) \to s(x)$ $\qquad$ (2) $S(\underline{1} \underline{+} u,x) \to s(S(u,x))$
(3) $S(u,S(v,x)) \to S(u \underline{+} v,x)$ $\qquad$ (4) $S(u,s(x)) \to s(S(u,x))$

Because of rule (4) the Theorem 5.1 does not apply. But if R consits of the rules (1) - (3), then R is confluent modulo A on the parameter-free $spec_2$-terms since every such a $spec_2$-term, which is not a $spec_1$-term, is R/A-reducible. So Theorem 5.1 applies and $spec_2$ is a consistent enrichment of $spec_1$.

Notice that this argument works also if we have $F_0 = \{S_1,\dots,S_n, \underline{1}, \underline{+}\}$ and the equations of E_0 with S replaced by S_i , $i = 1,\dots,n$.

Now we address another problem we have to solve for our method to work: Given a consistent enrichment $spec_2$ of $spec_1$ and an equation $t_1 = t_2$ of $spec_2$. Is $t_1 = t_2$ valid with respect to $spec_2$ and $spec_1$? In our applications it is very often the case that a parameter-free $spec_2$-term t is E_2-equal to at most one $spec_1$-term s. This leads to the following lemma which is directly a consequence of the definition of a valid equation.

Lemma 5.3:

Let $spec_2 = (\Sigma_1 \cup \Sigma_0, F_1 \cup F_0; E_1 \cup E_0)$ be a consistent enrichment of $spec_1 = (\Sigma_1, F_1; E_1)$. The equation $t_1 = t_2$ is valid with respect to $spec_2$ and $spec_1$ if for every parameter substitution ψ there are $spec_1$-terms s_1, s_2 such that $\psi(t_1) =_{E1 \cup E_0} s_1 =_{E1} s_2 =_{E1 \cup E_0} \psi(t_2)$. ■

As an example, let E_1 contain the equations

$$s(p(x)) = x \qquad p(s(x)) = x$$

and E_0 is

$$E_0: \quad s(x) = S(\underline{1},x) \qquad S(u,S(v,x)) = S(u \underline{+} v,\ x)$$
$$p(x) = P(\underline{1},x) \qquad P(u,P(v,x)) = P(u \underline{+} v,\ x)$$
$$\underline{+} \text{ is AC}$$

Then the following equations are valid

$$P(u,S(v,x)) = S(v,P(u,x))$$
$$S(u,P(u,x)) = x$$
$$S(u \underline{+} v,P(v,x)) = S(u,x)$$
$$S(u,P(u \underline{+} v,x)) = P(v,x)$$

Using these equations one can prove (along the lines in section 4) that $x + 0 = x$ is an inductive theorem of

$$E_1: \quad 0 + y = y \qquad s(p(x)) = x$$
$$s(x) + y = x + s(y) \qquad p(s(x)) = x$$
$$p(x) + y = x + p(y)$$

6. Examples

a) As a starting example we use

E_1: $a[b[a[x]]] = b[a[b[x]]]$

This is an example of Kapur and Narendran. They show in [KNa] that over the signature using $F_1 = \{a,b\}$ no finite convergent R for E_1 exists. We propose two extensions to get a convergent R for solving E_1-equality. Let us write aba[x] for a[b[a[x]]].
The first extension is an intelligent one, it uses a new function symbol c and the extension

E_2: $aba[x] = bab[x]$
$c[x] = ab[x]$

Clearly, the results of section 5 prove that $spec_2$ is a consistent enrichment of $spec_1$. Here we have no parameters. Completion of E_2 gives

R_2: $ab[x] \rightarrow c[x]$ $bcb[x] \rightarrow c^2[x]$
$ca[x] \rightarrow bc[x]$ $c^2b[x] \rightarrow ac^2$

The second extension uses the general method to finitely describe all $a^n[x]$ and $b^n[x]$. Starting the completion procedure with E_1 the following rules are produced

$aba[x] \rightarrow bab[x]$
$ab^{n+1}ab[x] \rightarrow bab^2a^n[x]$ $n \geq 1$

The first rule gives $aba^n[x] =_{E1} b^nab[x]$ for all $n \geq 0$. So we use the extension described by

E_0: $a[x] = A[\underline{1},x]$ $A[u,A,[v,x]] = A[u\underline{+}v,x]$
$b[x] = B[\underline{1},x]$ $B[u,B[v,x]] = B[u\underline{+}v,x]$
$\underline{+}$ is AC

and add the valid equations

$A[\underline{1},B[\underline{1}\underline{+}u,A[\underline{1},B[1,x]]]]] = B[\underline{1},A[\underline{1},B[\underline{1}\underline{+}\underline{1},A[u,x]]]]$
$A[\underline{1},B[\underline{1},A[u,x]]] = B[u,A[\underline{1},B[\underline{1},x]]]$

To enhence readability we write $A^u[x]$ instead of A[u,x]. With this notation the last equation becomes $A^1B^1A^u[x] = B^uA^1B^1[x]$.
Now completion leads to the finite convergent system

R: $a[x] \rightarrow A^1[x]$ $\quad A^u A^v[x] \rightarrow A^{u+v}[x]$

$b[x] \rightarrow B^1[x]$ $\quad B^u B^v[x] \rightarrow B^{u+v}[x]$

$\underline{+}$ is AC

$$A^1B^1A^u[x] \rightarrow B^uA^1B^1[x]$$
$$A^{1+v}B^1A^u[x] \rightarrow A^vB^uA^1B^1[x]$$
$$A^1B^{1+u}A^1B^1[x] \rightarrow B^1A^1B^{1+1}A^u[x]$$
$$A^1B^{1+u}A^1B^{1+w}[x] \rightarrow B^1A^1B^{1+1}A^uB^w[x]$$
$$A^{1+v}B^{1+u}A^1B^1[x] \rightarrow A^vB^1A^1B^{1+1}A^u[x]$$
$$A^{1+v}B^{1+u}A^1B^{1+w}[x] \rightarrow A^vB^1A^1B^{1+1}A^uB^w[x]$$

b) The second example is

E_1: $\quad hf^ng[x] = f^ng[x] \qquad n \geq 1$

$fg^mk[x] = g^mk[x] \qquad m \geq 1$

Here we start with two infinite sequences of equations. We use our general method and get

E_2: $\quad f[x] = F[\underline{1},x] \qquad F[u,F[v,x]] = F[u\underline{+}v,x]$

$g[x] = G[\underline{1},x] \qquad G[u,G[v,x]] = G[u\underline{+}v,x]$

$h[F[u,g[x]]] = F[u,g[x]]$

$f[G[u,k[x]]] = G[u,k[x]]$

Now completion stops with the relevant rules

$$hF^uG^1[x] \rightarrow F^uG^1[x]$$
$$F^1G^uk[x] \rightarrow G^uk[x]$$
$$h[G^1k[x] \rightarrow G^1k[x]$$
$$F^{1+u}G^vk[x] \rightarrow F^uG^vk[x]$$
$$hF^uG^{1+v}[x] \rightarrow F^uG^{1+v}[x]$$
$$hG^{1+v}k[x] \rightarrow G^{1+v}k[x]$$

c) The third example taken from Hermann [Her], Example 3.15, is artificial but technically more complex. Starting completion with

E_1: $\quad d[x+(x\cdot y)] = y$

$g[x]+y = g[x+f[x,y]]$

orients the two equations from left to right and produces the infinite set of rules

$$d[g[x+f[x,g[x]\cdot y]]] \rightarrow y$$
$$d[g^2[x+f[x,f[g[x],g^2[x]\cdot y]]] \rightarrow y$$
$$d[g^3[x+f[x,f[g[x],f[g^2[x],g^3[x]\cdot y]]]] \rightarrow y$$

. . .

Using $F[\underline{n},x,y] :\equiv f[x,f[g[x],\ldots,f[g^{n-1}[x],g^n[x]\cdot y]\ldots]]$, $G[\underline{n},x] :\equiv g^n[x]$ we get

E_2: E_1 and

$$f[x,g[x]\cdot y] = F[\underline{1},x,y]$$
$$F[\underline{1}\underline{+}u,x,y] = f[x,F[u,g[x],y]]$$
$$g[x] = G[\underline{1},x]$$
$$G[u,G[v,x]] = G[u\underline{+}v,x]$$
$$d[G[u,x+F[u,x,y]]] = y$$

The comletion procedure with input E_2 orients all the equations from left to right and stops successfully after generating the following three rules

$$f[G^v[x],G^{1+v}[x]\cdot y] \rightarrow F^1[G^v[x],y]$$
$$G^{1+v}[x]+y \rightarrow G^1G^v[x]+f[G^v[x],y]$$
$$f[G^v[x],F^u[G^{1+v}[x],y]] \rightarrow F^{1+u}[G^v[x],y]$$

d) As a last example we show how to prove inductive theorems on Binomi numbers b[i,j]. We use the specification $spec_1$ given by

E_1:

$$0+y = y$$
$$s[x]+y = s[x+y]$$
$$b[0,0] = 0$$
$$b[0,s[y]] = 0$$
$$b[s[x],0] = s[0]$$
$$b[s[x],s[y]] = b[x,s[y]] + b[x,y]$$

and want to prove that $E \subseteq ITh[E_1]$ for

E: $b[x,x] = s[0]$ $\qquad$ $b[x,s[x]] = 0$

Starting the completion process with input $E_1 \cup E$ it diverges and produces the terms $s^n[x]$. So we use the extension described by

E_0:

$$s[x] = S[\underline{1},x]$$
$$S[u,S[v,x]] = S[u\underline{+}v,x]$$
$$\underline{+} \text{ is AC}$$

Again, the completion process with input $E_1 \cup E_0 \cup E$ diverges now producing $b[x,S[\underline{1}\underline{+}\ldots\underline{+}1,x]] = 0$. So we add as inductive hypotheses the equation

$$b[x,S[u,x]] = 0$$

Now the completion procedure stops with

R:	$s[x] \to S^1[x]$	$S^u S^v[x] \to S^{u \underline{+} v}[x]$
	$0+y \to y$	$S^1[x]+y \to S^1[x+y]$
	$b[0,0] \to 0$	$S^{1+v}[x]+y \to S^1[S^v[x]+y]$
	$b[0,S^1[x]] \to 0$	$b[0,S^{1+v}[x]] \to 0$
	$b[S^1[x],0] \to S^1[x]$	$b[S^{1+v}[x],0] \to S^1[0]$
	$b[S^1[x],S^1[y]] \to b[x,S^1[y]]+b[x,y]$	
	$b[S^{1+v}[x],S^1[y]] \to b[S^v[x],S^1[y]+b[S^v[x],y]$	
	$b[S^1[x],S^{1+v}[y]] \to b[x,S^{1+v}[y]]+b[x,S^v[y]]$	
	$b[S^{1+u}[x],S^{1+v}[y]] \to b[S^u[x],S^{1+v}[y]]+b[S^u[x],S^v[y]]$	
	$b[x,x] \to S^1[0]$	
	$b[x,S^u[x]] \to 0$	
	$b[S^v[x],S^{u \underline{+} v}[x]] \to 0$	
	$\underline{+}$ is AC	

Let R_2 denote the rewrite system R with the last three rules eliminated. Then the specification described by R_2 is a consistent enrichment of that described by E_1. The left hand sides of the last three rules are R_2/AC-reducible, so these last three (directed) equations are inductive theorems of E_1. This proves $E \subseteq ITh(E_1)$.

References

[AMa] Avenhaus, J., Madlener, K.: Term rewriting and equational reasoning, to appear in R.B. Banerji: Formal techniques in Artificial Intelligence: A source book Elsevier, Amsterdam, 1989

[Bac] Bachmair, L.: Proof by consistency in equational theories, 3rd. LICS (1988), pp. 228-233

[BDe] Bachmair, L., Dershowitz, N.: Completion for rewriting modulo a congruence, TCS 67 (1989), pp. 173-201

[BDP] Bachmair, L., Dershowitz, N., Plaisted, D.: Completion without Failure, Coll. on the Resolution of Equations in Algebraic Structures, Austin (1987), Academic Press, NY 1989

[BKR] Benninghofen, B., Kemmerich, S., Richter, M.M.: Systems of Reductions, LNCS 277, Springer, Berlin (1987)

[Der] Dershowitz, N.: Termination, J. Symb. Comp. 3(1987), pp. 69-116

[Fri] Fribourg, L.: A strong restriction of the inductive completion procedure, 13th ICALP (1986), LNCS 226, pp. 105-115.

[Göb] Göbel, R.: A completion procedure for generating ground confluent term rewriting systems, Dissertation, U. Kaiserslautern (Germany) 1987, partially in Ground Confluence, 2nd RTA (1987), LNCS 256, pp. 156-167.

[Her] Hermann, M.: Vademecum of divergent term rewriting systems, Research Report 88-R-082, Centre de Recherche en Informatique de Nancy, 1988

[Hue] Huet, G.: Confluent reductions: Abstract properties and applications to term rewriting systems, J. ACM 27 (1980), pp. 797-821.

[JKi] Jouannaud, J.P., Kirchner, H.: Completion of a set of rules modulo a set of equations, SIAM J. Comp. 15 (1986), pp. 1155-1194

[JKo] Jouannaud, J.P., Kounalis, E.: Automatic proofs by induction in theories without constructors, Inf. and Comp. 82 (1989), pp. 1-33

[KNa] Kapur, D., Narendran, P.: A finite Thue system with decidable word problem and without equivalent finite canonical system, Theoret. Comput. Sci. 35 (1985), pp. 337-344.

[KBe] Knuth, D.E., Bendix, P.B.: Simple word problems in universal algebras, Computational problems in abstract algebra (ed.): J. Leech, Pergamon Press (1970), pp. 263-297.

[Kir] Kirchner, H.: Schematization of infinite sets of rewrite rules generated by divergent completion processes, TCS 67 (1989), pp. 303-332

[Kue] Küchlin, W.: Inductive completion by ground proof transformation. Coll. on the Resolution of Equations in Algebraic Structures, Austin 1987, Academic Press, NY (1989)

[Lan] Lange, St.: Towards a set of inference rules for solving divergence in Knuth-Bendix completion, in K.P. Jantke (ed.): Analogical and inductive inference, LNCS 397 (1989), pp. 304-316

[PSt] Peterson, G.E., Stickel, M.E.: Complete sets of reduction for some equational theories, J. ACM 28 (1981), pp. 233-264

[TJa] Thomas, M., Jantke, K.P.: Inductive inference for solving divergence in Knuth-Bendix completion, in K.P. Jantke (ed.): Analogical and inductive inference, LNCS 397 (1989), pp. 288-303