Effective codescent morphisms in the varieties determined by convergent term rewriting systems

Guram Samsonadze[1] and Dali Zangurashvili[2]

[1]Georgian Technical University, 77 Kostava Str., Tbilisi 0175, Georgia
[2] A. Razmadze Mathematical Institute, Tbilisi Centre for Mathematical Sciences, 6 Tamarashvili Str., Tbilisi 0177, Georgia

E-mail: [1]g.samsonadze@gtu.ge, [2]dalizan@rmi.ge

Abstract

It is shown that the elements of amalgamated free products in a variety of universal algebras have unique normal forms if the variety is represented by a confluent term rewriting system satisfying some additional requirements for its signature and rules. Applying this fact it is proved that any codescent morphism is effective in such varieties. In particular, this is the case for the variety of Mal'tsev algebras, the varieties of magmas with unit and two-sided inverses, idempotent quasigroups, unipotent quasigroups, left Steiner loops, and right Steiner loops.

1 Introduction

This paper continues the study of the problem of describing effective codescent morphisms in varieties of universal algebras which was posed by G. Janelidze. The study is carried out employing the term rewriting systems techniques.

In a number of works it was proved that every codescent morphism is effective in some concrete varieties. Namely, besides the trivial cases, this fact was established for commutative rings with unit (Joyal-Tierney (unpublished), Mesablishvili [16], Janelidze-Tholen [12]), Boolean algebras (Makkai (unpublished)), groups (Zangurashvili [20], [21]). The recent paper [21] gives the sufficient condition formulated in the syntactical form, for all codescent morphisms of a variety satisfying the amalgamation property to be effective. Applying this result it is proved there that codescent morphisms are effective in varieties of (left/right) quasigroups, loops and magmas. Moreover, it is shown that the problem is closely related to the question whether the elements of amalgamated free products have unique normal forms (for the precise definition of the notion "normal form" we refer the reader to Section 3).

In this paper we relate this question to the notion of confluency, which is one of the central notions of the term rewriting systems theory. Namely, we show that the elements of amalgamated free products have unique normal forms in any variety represented by a confluent term rewriting system which satisfies some additional conditions of syntactical nature. Namely, it is assumed that, for any rule $l \rightarrow r$ from Σ, no variable occurs in r more often than in l; the size of the term l is greater than the size of the term r; for any subterm l' of l which is neither a variable nor a constant, any variable occuring in l occurs in l' too; and, finally, the signature contains no more than one constant [*]. In passing, the proven result implies that varieties of the mentioned kind satisfy the

---

[*]In fact, a weaker condition is required.

strong amalgamation property in the sense of [13], and that the word problem for the elements of amalgamated free products of a finite number of finite algebras is decidable.

Applying the obtained result on the unique normal forms for the elements of amalgamated free products, we prove that all codescent morphisms are effective in the variety represented by a confluent term rewriting system satisfying the above syntactical conditions. This implies that codescent morphisms are effective in the variety of Mal'tsev algebras, the varieties of magmas with unit and two-sided inverses, idempotent quasigroups, unipotent quasigroups, left Steiner loops, and right Steiner loops.

It is not required of the reader to be familiar with the term rewriting systems theory – a small introduction to the main concepts of this theory is given in the next section.

2   Preliminaries

All the definitions and facts given in this section can be found in [1], unless specified otherwise.

2.1   Confluent binary relations

Let A be a set, and let $\to$ be a binary relation on A. Let $\xrightarrow{*}$ be the reflexive transitive closure of $\to$, and $\leftrightarrow$ be the symmetric closure of $\to$. In particular, $\xleftrightarrow{*}$ is the smallest equivalence relation containing $\to$.

An element a of A is called *reducible* if there is $b \in A$ such that $a \to b$. In that case we say that b is obtained by reducing a. a is said to be in *normal form* (or *irreducible*) if it is not reducible. b is called a normal form of a if $a \xrightarrow{*} b$ and b is in normal form. Elements a and b are called joinable if there is an element c such that $a \xrightarrow{*} c \xleftarrow{*} b$, in which case we write $a \downarrow b$.

A relation $\to$ is called *terminating* if there is no infinite sequence $a_0 \to a_1 \to \dots$. The equivalent condition is that the relation $\to$ is *well-founded*. Recall that this means that every nonempty subset B of A has a $\to$-minimal element, i.e. an element $a \in B$ such that there is no $b \in B$ with $b \to a$.

A relation $\to$ is called *confluent* (resp. *semi-confluent*; *locally confluent*) if any elements a and b with $a \xleftarrow{*} c \xrightarrow{*} b$ (resp. $a \leftarrow c \xrightarrow{*} b$; $a \leftarrow c \to b$) for some c, are joinable.

A relation $\to$ is said to satisfy the *Church-Rosser property* if any elements a and b with $a \xleftrightarrow{*} b$ are joinable.

A relation $\to$ is called *convergent* if it is both terminating and confluent.

A relation $\to$ is called *normalizing* if every element has a normal form.

The following lemma is obvious.

Lemma 2.1. A terminating relation is normalizing.

We have

Theorem 2.2. The following conditions are equivalent:
   (i) a relation $\to$ satisfies the Church-Rosser property;
   (ii) a relation $\to$ is confluent;
   (iii) a relation $\to$ is semi-confluent.
   If a relation $\to$ is terminating, then these conditions are equivalent also to each of the following ones:
   (iv) a relation $\to$ is locally confluent;
   (v) every element of A has a unique normal form.

For the proof of the equivalence of the conditions (i)-(iii) we refer the reader to [1]. The equivalence of (ii) and (iv) is exactly the essence of Newman's lemma [17], [1], while the equivalence of (ii) and (v) is obvious.

2.2   Terms and Substitutions

Let $\mathfrak{F}$ be a signature, i.e., a set of operation symbols equipped with arities, and let X be a denumerable set such that $\mathfrak{F} \cap X = \varnothing$. Unless specified otherwise, we will use "term" to mean a $\mathfrak{F}$-term over X.

The structure of a term can be illustrated by representing it as a tree, where the operation symbols and the variables are nodes and the arrows connect the operation symbols with their arguments. Using the standard numbering of the nodes of a tree by strings of positive integers, to each occurrence of an operation symbol and a variable in a term one can relate such a string, called a *position* of the term. For instance, the term $t = f(f(x, f(x, x)), f(c, x))$, where c is a constant and f is a binary operation symbol can be presented as the following tree; the strings of positive integers are the positions assigned to the tree nodes (e is the empty string).

(2.1)
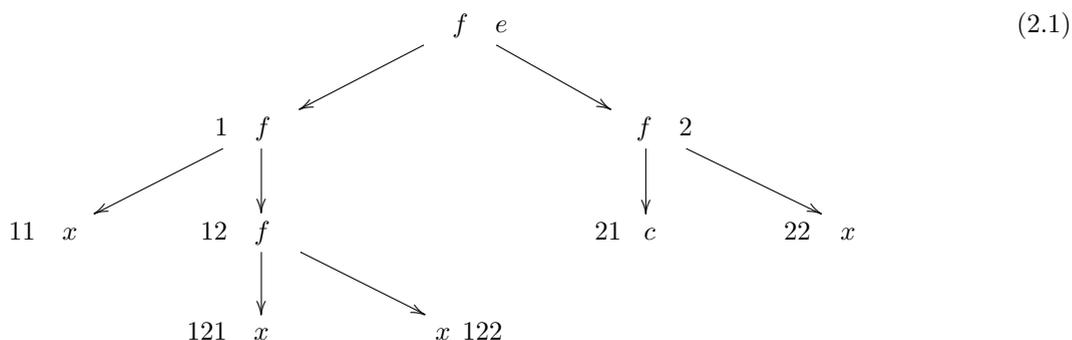
For the set $Pos(t)$ of positions of t we have

– if $t = x \in X$, then $Pos(t) = \{e\}$;
– if $t = f(t_1, t_2, ..., t_n)$, then $Pos(t) = \{e\} \bigcup \bigcup_{i=1}^{n} \{ip | p \in Pos(t_i)\}$.

The position e is called the *root position* of the term t.

The cardinality of $Pos(t)$ is called the *size* of t.

A term is called *ground* if it does not contain any variable.

Let t be a term. For $p \in Pos(t)$, the subterm of t at the position p, denoted by $t|_p$, is defined by the induction with respect to the length of p:

$$t|_e = t;$$

$$f(t_1, t_2, ..., t_n)|_{iq} = t_i|_q.$$

The tree of a subterm of t is obviously a subtree of the tree of t.

Let t' be also a term. For $p \in Pos(t)$, we denote by $t[t']_p$, the term which is obtained from t by replacing the subterm at the position p by t', i.e.,

$$t[t']_e = t';$$

$$f(t_1, t_2, ..., t_n)[t]_{iq} = f(t_1, t_2, ..., t_i[t']_q, ..., t_n).$$

For instance, for the term in the figure (2.1), we have $Pos(t) = \{e, 1, 2, 11, 12, 21, 22, 121, 122\}$. The subterm at the position $p = 12$ is $t|_p = f(x, x)$. If $t' = f(c, f(x, c))$, then $t[t']_p = f(f(x, f(c, f(x, c))), f(c, x))$.

For a finite set of terms $t_1, t_2, ..., t_n$, we denote by $Var(t_1, t_2, ..., t_n)$ the set of variables occurring in at least one of them.

Let $T(\mathfrak{F}, X)$ be the set of all terms. A *substitution* is defined as a mapping $\sigma : X \to T(\mathfrak{F}, X)$ such that the set $\{x | \sigma(x) \neq x\}$ is finite. This set is called the *domain* of σ and denoted by $Dom(\sigma)$. The *range* of σ is defined as the set $Ran(\sigma) = \{\sigma(x) | x \in Dom(\sigma)\}$.

A *renaming* is defined as an injective substitution ϱ such that $Ran(\varrho) \subset X$.

Recall that $T(\mathfrak{F}, X)$ has the structure of an $\mathfrak{F}$-algebra, and moreover, is free over the set X. Hence the mapping σ can be extended to the unique $\mathfrak{F}$-homomorphism $\hat{\sigma} : T(\mathfrak{F}, X) \to T(\mathfrak{F}, X)$. Namely, $\hat{\sigma}$ simultaneously replaces all occurrences of variables in a term by their images under the mapping σ.

The *composition* $\sigma\tau$ of two substitutions σ and τ is defined as the mapping $\hat{\sigma}\tau$ (which obviously is a substitution).

A substitution σ is called *more general* than a substitution τ if there exists a substitution δ such that $\tau = \delta\sigma$.

Let t and t' be terms. A substitution σ is called a *unifier* of these terms if $\sigma(\hat{t}) = \hat{\sigma}(t')$. We say that the terms t and t' unify if there exists such a substitution.

A unifier σ of terms t and t' is called the *most general unifier* if it is more general than any unifier of these terms.

Theorem 2.3. If terms t and t' unify, then there exists the most general unifier. Moreover, it is unique up to a renaming (i. e., if σ and σ' are most general unifiers of these terms, then there exists a renaming ϱ such that $\sigma = \rho\sigma'$).

In fact, there exists an algorithm for finding the most general unifier. Moreover, there are several such algorithms differing from one another in their efficiency (see, for instance, [3],[9], [15],[18]).

2.3   Term Rewriting Systems

The term rewriting systems theory deals with transformations of terms using a set of identities, for various goals. However, as different from universal algebra, the identities here can be used only in one direction (say, from left to right).

Let X be a denumarable set of variables, and Σ be a set of $\mathfrak{F}$-identities. **Throughout the paper all identities from Σ are assumed to be oriented.**

The pair $(\mathfrak{F}, \Sigma)$ is called a *term rewriting system* if, for any identity $l = r$ from Σ, l is not a variable and $Var(l) \supset Var(r)$.

Consider the following binary relation $\rightarrow_{(\mathfrak{F},\Sigma)}$ on the set $T(\mathfrak{F}, X)$ of terms over the set X:

$$t \rightarrow_{(\mathfrak{F},\Sigma)} t'$$

if the following condition is satisfied:

(C) there exist an identity (l, r) from Σ, a substitution σ and a position p of t such that $t|_p = \hat{\sigma}(l)$ and $t' = t[\hat{\sigma}(r)]_p$.

This relation is called the *reduction relation* defined by $(\mathfrak{F}, \Sigma)$. We say that terms have *unique normal forms* if they have unique normal forms with respect to the reduction relation.

The well-known Birkhoff's Theorem asserts that the equality $t = t'$ holds in any algebra from the variety of universal algebras determined by $(\mathfrak{F}, \Sigma)$ if and only if $t \overset{*}{\leftrightarrow}_{(\mathcal{F},X)} t'$. There is also another characterization of $\overset{*}{\leftrightarrow}_{(\mathcal{F},X)}$, by which $\overset{*}{\leftrightarrow}_{(\mathcal{F},X)}$ is the smallest congruence on $T(\mathfrak{F}, X)$ which contains Σ and is closed under substitutions.

A term rewriting system $(\mathfrak{F}, \Sigma)$ is called *terminating* (resp. *confluent*; *locally confluent*; *convergent*) if the reduction relation $\rightarrow_{(\mathfrak{F},\Sigma)}$ is of the same kind.

The problems, when a term rewriting system is terminating and when it is confluent are the central ones in the term rewriting systems theory. Below we give some well-known relevant results.

It is obvious that if no variable occurs in the right-hand side more often than in the left-hand side (such identities are called *duplicating*) and, moreover, the size of the left-hand side of any identity is greater than the size of its right-hand side, then the term rewriting system is terminating. Much stronger result is known. To formulate it, we first give the following definition.

A binary relation $>$ on the set of terms $T(\mathfrak{F}, X)$ is called a *reduction order* if it is transitive, irreflexive, well-founded, closed under substitutions, and compatible with $\mathfrak{F}$-operations (i.e., for any $s_1, s_2 \in T(\mathfrak{F}, X)$, for any $n \geq 1$, and any n-ary operation symbol $f \in \mathfrak{F}$, if $s_1 > s_2$, then $f(t_1, t_2, ..., t_{i-1}, s_1, t_{i+1}, ..., t_n) > f(t_1, t_2, ..., t_{i-1}, s_2, t_{i+1}, ..., t_n)$, for any i $(1 \leq i \leq n)$ and any $t_1, t_2, ..., t_{i-1}, t_{i+1}, ..., t_n \in T(\mathfrak{F}, X))$.

For instance, the relation $>$, where $t_1 > t_2$ if the size of t_1 is greater than the size of t_2, is not closed under substitutions, in general. However, if none of the identities from Σ is duplicating, then it is closed, and moreover, $>$ is a reduction order.

Theorem 2.4. A term rewriting system $(\mathfrak{F}, \Sigma)$ is terminating if and only if there exists a reduction order $>$ that satisfies $l > r$ for all identities $l = r$ from Σ.

Let

$$l_1 = r_1, l_2 = r_2 \tag{2.2}$$

be identities from Σ. Let us rename their variables so that

$$Var(l_1, r_1) \bigcap Var(l_2, r_2) = \varnothing. \tag{2.3}$$

Let p be a position of l_1 such that $l_1|_p$ is not a variable and the terms $l_1|_p$ and l_2 unify (in that case one says that the term l_1 *overlaps* the term l_2 at the position p). Let σ be the most general unifier of $l_1|_p$ and l_2. The pair of terms $(\hat{\sigma}(r_1), \hat{\sigma}(l_1)[\hat{\sigma}(r_2)]_p)$ is called a *critical pair* determined by the identities (2.2). Note that the term $\hat{\sigma}(l_1)$ is in the relation $\rightarrow_{(\mathfrak{F},\Sigma)}$ with both terms participating in the critical pair:

$$\hat{\sigma}(l_1) \tag{2.4}$$

$$\hat{\sigma}(r_1) \qquad\qquad \hat{\sigma}(l_1)[\hat{\sigma}(r_2)]_p$$

Let us assume that (2.3) is satisfied for any distinct identities (2.2) from Σ (after renaming the variables, if necessary).

Theorem 2.5. The following conditions are equivalent:

(i) the relation $\rightarrow_{(\mathfrak{F},\Sigma)}$ is locally confluent;

(ii) all critical pairs determined by all pairs of identities (2.2) from Σ (including the pair of any identity and its renamed copy) are joinable.

If the relation $\rightarrow_{(\mathfrak{F},\Sigma)}$ is terminating, then these conditions are equivalent also to the condition:

(iii) the relation $\rightarrow_{(\mathfrak{F},\Sigma)}$ is confluent;

(iv) every term from $T(\mathfrak{F}, X)$ has a unique normal form;

(v) for any critical pair (u_1, u_2), and any normal forms $\underline{u_1}$ and $\underline{u_2}$ of resp. u_1 and u_2, one has $\underline{u_1} = \underline{u_2}$.

Remark 2.6. If Σ is finite and the term rewriting system is normalizing, then obviously the condition (v) can be verified in a finite number of steps.

Recall that one says that the word problem is decidable for $(\mathfrak{F}, \Sigma)$ if there is an algorithm which gives, in a finite number of steps, the answer to the question whether the equality $t = t'$ holds in any algebra of the variety represented by $(\mathfrak{F}, \Sigma)$, for any terms t and t'.

Corollary 2.7. If Σ is finite and $(\mathfrak{F}, \Sigma)$ is convergent, then the word problem is decidable.

Remark 2.8. It is obvious that for any critical pair (u_1, u_2) the identity $u_1 = u_2$ holds in any algebra from the variety determined by a term rewriting system $(\mathfrak{F}, \Sigma)$. Therefore if the terms u_1 and u_2 in the critical pair are not joinable, one can make them joinable by adding the identity $u_1 = u_2$ or $u_2 = u_1$ to the set of identities. However, the new critical pairs might then arise. Repeating this process sufficiently many times one might (or might not) obtain a locally confluent system which represents the same variety. This approach is used in the so-called completion procedures introduced by Knuth-Bendix in [14] for constructing convergent representations of varieties, and further developed in [2],[4], [7], [10] and a lot of other papers.

Example 2.9. Consider the variety of magmas with unit and two-sided inverses. Let us denote the binary operation by f, the inverse's operation by u and the unit by 1. Then the identities take the form

$$f(x, 1) = x, \tag{2.5}$$

$$f(1, x) = x, \tag{2.6}$$

$$f(u(x), x) = 1, \tag{2.7}$$

$$f(x, u(x)) = 1. \tag{2.8}$$

This system is not confluent since the critical pair obtained by overlapping the left-hand sides of the identity (2.5) with the renamed copy $f(u(y), y) = 1$ of the identity (2.7) is not joinable. Indeed, the most general unifier σ of $f(x, 1)$ and $f(u(y), y)$ is the substitution $x \mapsto u(1)$, $y \mapsto 1$ (and being identical at all other variables), so that the corresponding critical pair is $(u(1), 1)$.

$$f(u(1), 1)$$

$$u(1) \qquad\qquad\qquad 1$$
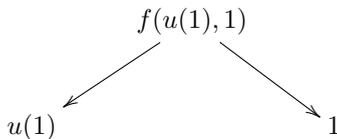
It is obvious that this critical pair is not joinable. However, if we add the identity

$$u(1) = 1 \tag{2.9}$$

to the above list of identities, this critical pair will obviously become joinable. One easily can verify that all other (previous and new) critical pairs are joinable with respect to the extended system (2.5)-(2.9), and, since the system is terminating, it is confluent by Theorem 2.5.

3   Amalgamated free products

From now on, we will assume that $\mathcal{C}$ is the variety of universal algebras of type $\mathfrak{F}$ defined by a set Σ of identities, and the following condition is satisfied:

(*) *none of the identities from Σ is duplicating, and, moreover, for each identity $l = r$ from Σ the size of the term l is greater than the size of the term r.*

The condition (*) in particular implies that $(\mathfrak{F}, \Sigma)$ is a term rewriting system.

Let I be a set, B and A_i $(i \in I)$ be algebras from $\mathcal{C}$ such that, for any i, B is a subalgebra of A_i, and

$$A_i \cap X = A_i \cap \mathfrak{F}_{\mathbf{o}} = \emptyset, \tag{3.1}$$

where $\mathfrak{F}_{\mathbf{o}}$ is the set of constants of $\mathfrak{F}$. For simplicity, it is assumed that

$$A_i \cap A_j = B, \tag{3.2}$$

for any distinct i, j.

In the set of terms over the set $\underset{i \in I}{\cup} A_i$ we introduce the binary relation $\to$ as follows:

$$t \to t'$$

if either the condition (**C**) or the condition (**C1**) below is satisfied:

(**C1**) the term t contains a subterm

$$f(a_1, a_2, ..., a_n) \tag{3.3}$$

at some position $p \in Pos(t)$, with f being an n-ary operation and $a_1, a_2, ..., a_n$ being variables from one and the same A_i, and, moreover, $t[a]_p = t'$, where a is the value of $f(a_1, a_2, ..., a_n)$ in A_i.

It is well known that the free product A of $(A_i)_{i \in I}$ with the amalgamated subalgebra B is isomorphic to the quotient of the (not necessarily $\mathcal{C}$-)algebra of terms over the set $\underset{i \in I}{\cup} A_i$ of variables with respect to the congruence R, where a term t is R-equivalent to a term t' if and only if either $t = t'$ or there exists a sequence of terms $t_1, t_2, ..., t_n$ such that $t_1 = t$, $t_n = t'$, and, for any i ($1 \le i \le n-1$), either $t_i \to t_{(i+1)}$ or $t_{(i+1)} \to t_i$. In other words, R coincides with the equivalence relation $\overset{*}{\leftrightarrow}$.

The condition (*) implies that the relation $\to$ is terminating. Therefore any element of the amalgamated free product has a representative (called the *normal form* of this element) which is irreducible with respect to $\to$. A question that arises now is when normal forms are unique.[†] It was shown in [6] that this is the case for varieties of (left/right)quasi-groups, loops, and magmas.

From Theorem 2.2 follows

Proposition 3.1. The following conditions are equivalent:
   (i) the elements of amalgamated free products have unique normal forms;
   (ii) terms over the set $\underset{i \in I}{\cup} A_i$ have unique normal forms with respect to the relation $\to$;
   (iii) the relation $\to$ is confluent.

We are now going to construct a term rewriting system induced by $(B, (A_i)_{i \in I})$. But first we impose the following condition on $(\mathfrak{F}, \Sigma)$:

(**) *If the set $\mathfrak{F}_\circ$ of constants is not empty, then, for any non-trivial algebra C from the variety $\mathcal{C}$, the mapping $\mathfrak{F}_\circ \to C$ sending a constant to its value in C is injective.*

Let us extend the set of constants $\mathfrak{F}_\circ$ to the set $\cup_{i \in I} A_i$ (identifying constants from $\mathfrak{F}_\circ$ with the corresponding elements of B). We denote the set of operations obtained in this way by $\mathfrak{F}'$. Moreover, for any natural n, any $a_1, a_2, ..., a_n \in A_i$, and any n-ary operation symbol f, we add the identity

$$f(a_1, a_2, \ldots, a_n) = a \tag{3.4}$$

to the set Σ, where a is the value of $f(a_1, a_2, ..., a_n)$ in A_i. We denote the extended set of identities by Σ'.

It is obvious that the set of terms over $\underset{i \in I}{\cup} A_i$ is equal to the subset $T(\mathfrak{F}', \varnothing)$ of ground terms of $T(\mathfrak{F}', X)$. The following lemma is obvious.

[†]Note that the meaning of "a normal form" as given here is different from that used in [21]. An irreducible representative is called the normal form in [21] if it is unique. Accordingly, "a variety with normal forms for the elements of amalgamated free products" in the sense of [21] and "a variety with *unique* normal forms for the elements of amalgamated free products" is the sense of the present paper are equivalent notions.

Lemma 3.2. If all constants contained in a ground term $t \in T(\mathfrak{F}', \varnothing)$ belong to one and the same A_i, and if the value of that term is a in A_i, then the terms a and t are joinable with respect to $\to_{(\mathfrak{F}', \Sigma')}$.

The condition (*) implies

Lemma 3.3. If $t \overset{*}{\to}_{(\mathfrak{F}', \Sigma')} t'$ and t is ground, then so is t'.

Lemma 3.4. $\to_{(\mathfrak{F}', \Sigma')} \bigcap (T(\mathfrak{F}', \varnothing) \times T(\mathfrak{F}', \varnothing)) = \to$.

Lemma 3.3 and Lemma 3.4 imply

Proposition 3.5. If the term rewriting system $(\mathfrak{F}', \Sigma')$ is confluent, then the relation $\to$ is also confluent.

Propositions 3.1 and 3.5 give rise to the idea of applying Theorem 2.5 to the term rewriting system $(\mathfrak{F}', \Sigma')$, when studying the question whether the elements of amalgamated free products have unique normal forms. However, this idea is not fruitful, since Σ' is infinite, in general, even if $\mathfrak{F}$ and Σ are finite. To be able to apply the algorithmic approach suggested by Theorem 2.5 to the question, we reduce the problem to the corresponding one for $(\mathfrak{F}, \Sigma)$. To this end, let us assume that one more condition is satisfied:

(***) *for any identity $l = r$ from Σ, any subterm l' of l which is neither a variable nor a constant, we have $Var(l') = Var(l)$.*

In particular, this condition implies that if l contains a binary operation symbol, then l contains no more than two different variables.

Lemma 3.6. Terms t and t' from $T(\mathfrak{F}, X)$ unify with respect to $\mathfrak{F}$ if and only if they unify with respect to $\mathfrak{F}'$. In that case, their most general unifiers with respect to these two signatures coincide up to a renaming.

Proof. The "only if" part is obvious. For the "if" part, assume that $\sigma(t) = \sigma(t')$ for some substitution σ with respect to $\mathfrak{F}'$. Choose a subset X' of X bijective to $(\mathfrak{F}'_\circ \setminus \mathfrak{F}_\circ) \bigcap \sigma(Var(t, t'))$ and disjoint with $Var(t, t')$. Consider the substitution θ, which maps a variable $x \in Var(t, t')$ to the term obtained from $\sigma(x)$ by replacing constants from $(\mathfrak{F}'_\circ \setminus \mathfrak{F}_\circ)$ in it by the corresponding elements of X'. Obviously, θ is a substitution with respect to $\mathfrak{F}$, and, since neither t nor t' contains constants from $(\mathfrak{F}'_\circ \setminus \mathfrak{F}_\circ)$, we have $\theta(t) = \theta(t')$.

Assume that σ is the most general unifier of t and t' with respect to $\mathfrak{F}$, and σ' is the most general unifier of these terms with respect to $\mathfrak{F}'$. Then $\sigma = \delta\sigma'$ for some substitution δ with respect to $\mathfrak{F}'$. Therefore if $\sigma'(x)$ contains an element c from $(\mathfrak{F}'_\circ \setminus \mathfrak{F}_\circ)$, for some $x \in Var(t, t')$, then, obviously, $\sigma(x)$ also contains c, which is impossible. This implies that σ' is a substitution with respect to $\mathfrak{F}$ too, and hence is the most general unifier with respect to $\mathfrak{F}$. Now it suffices to apply Theorem 2.3.   Q.E.D.

Proposition 3.7. If the term rewriting system $(\mathfrak{F}, \Sigma)$ is confluent, then so is $(\mathfrak{F}', \Sigma')$.

Proof. The term rewriting system $(\mathfrak{F}', \Sigma')$ is obviously terminating. According to Theorem 2.5, it suffices to show that any critical pair is joinable. This fact follows from Lemma 3.6 for the case where a critical pair is determined by arbitrary two identities from Σ. Besides, there are no nontrivial critical pairs in the case where both identities of Σ' are of the form (3.4).

Consider a critical pair determined by an identity of the form (3.4) and an identity $l = r$ from Σ. Since the size of l can not be 1, the overlap can occur only in the root position. Hence l has the form $f(x_1, x_2, ...x_n)$. Then the critical pair has the form $(a, \hat{\sigma}(r))$, for the substitution σ with $x_1 \mapsto a_1$, $x_2 \mapsto a_2$,..., $x_n \mapsto a_n$. The condition (*) implies that $\hat{\sigma}(r)$ is a ground term and does not contain constants other than $a_1, a_2, ..., a_n$. Since A_i is an algebra from $\mathcal{C}$, the identity $l = r$ holds in A_i, and hence we have the equalities $a = f(a_1, a_2, ..., a_n) = \hat{\sigma}(l) = \hat{\sigma}(r)$ in A_i. Lemma 3.2 implies that a and $\hat{\sigma}(r)$ are joinable with respect to $\rightarrow_{(\mathfrak{F}', \Sigma')}$.

Finally, let us consider the case where a critical pair is determined by an identity $l = r$ from Σ and the identity (3.4). If the overlap occurs at the position p, then $l|_p$ has the form $f(x_1, x_2, ..., x_n)$. The condition (***) implies that $Var(l) = \{x_1, x_2, ..., x_n\}$, and hence $\hat{\sigma}(l)$ is a ground term which contains only the constants $a_1, a_2, ..., a_n$, where σ is the most general unifier of $l|_p$ and (3.4). Then $\hat{\sigma}(l)$ is a term over A_i, and its value is equal to both the value of $\hat{\sigma}(r)$ and the value of $\hat{\sigma}(l)[a]_p$, for an element a in (3.4). Now it suffices to apply Lemma 3.2.   Q.E.D.

We obtain

Theorem 3.8. If a variety is represented by a confluent term rewriting system $(\mathfrak{F}, \Sigma)$ satisfying the conditions (*)-(***), then the elements of amalgamated free products have unique normal forms.

Corollary 3.9. Let a variety satisfy the conditions of Theorem 3.8. Let B be an algebra, $(A_i)_{i \in I}$ be a family of algebras such that there are embeddings $\alpha_i : B \rightarrowtail A_i$. Let A be the free product of $(A_i)_{i \in I}$ with the amalgamated subalgebra B and let $\beta_i : A_i \to A$ be the canonical homomorphisms. Then all β_i are monomorphic and, moreover, for any different $i, j \in I$, we have

$$\beta_i(A_i) \bigcap \beta_j(A_j) = \beta_i \alpha_i(B).$$

In particular, any variety of such kind satisfies the strong amalgamation property in the sense of [13].

Proof. It suffices to observe that the term a is in normal form, for any element a from $\bigcup_{i \in I} A_i$.   Q.E.D.

One says that the word problem for the free products of algebras $(A_i)_{i \in I}$ with an amalgamated subalgebra B is decidable if there is an algorithm which gives, in a finite number of steps, the answer to the question whether the elements of the amalgamated free product presented by any two terms over the set $\bigcup_{i \in I} A_i$ are equal. From Proposition 3.7 and Corollary 2.7 we obtain

Corollary 3.10. If I is finite and all algebras A_i are finite, then the word problem for the free product of these algebras with an amalgamated subalgebra B is decidable.

4   Some Examples

In this section we give examples of varieties satisfying the conditions of Theorem 3.8. Since some identities participating in their representations are the weak versions of the associativity/distributivity axioms, we write them, as well as some other ones in the traditional, and not in the term form as we have done so far.

Example 4.1. The confluency of the following systems is mentioned in [1] and can be easily verified.

(i) Let $\mathfrak{F}$ consist of one ternary operation symbol p and Σ consist of two Mal'tsev identities

$$p(x, x, y) = y,$$

$$p(x, y, y) = x.$$

For the convenience of referring, in this paper we call algebras from this variety Mal'tsev algebras.

(ii) Let k and n be natural numbers, and let $n > k$. Let $\mathfrak{F}$ consist of one unary operation symbol f and Σ consist of one identity

$$\underbrace{f(f(f(...f(}_{n \ times} x))) = \underbrace{f(f(f(...f(}_{k \ times} x)))$$

.

(iii) Let $\mathfrak{F}$ consist of two unary operation symbols f and g and Σ consist of the following identities:

$$f(f(x)) = f(x),$$
$$f(g(x)) = g(x),$$
$$g(g(x)) = f(x),$$
$$g(f(x)) = g(x).$$

(iv) Let $\mathfrak{F}$ consist of three unary operation symbols f, g and h, and Σ consist of two identities:

$$f(g(x)) = f(x),$$
$$g(h(x)) = h(x).$$

Example 4.2. Assume that the set of operations $\mathfrak{F}$ can be partitioned into two sets $\mathfrak{F}_c$ and $\mathfrak{F}_d$ such that the left-hand side of any identity from Σ has the form $f(t_1, t_2, ..., t_n)$ with $f \in \mathfrak{F}_d$ and $t_i \in T(\mathfrak{F}_c, X)$ (such a term rewriting system is called a *constructor* in the theory of such systems). If all f's are different, then such a system is locally confluent by Theorem 2.5. A simple example of a constructor is the system with two binary operation symbols $+$ and $\cdot$, one constant 0 and one identity

$$x \cdot y + y \cdot x = 0.$$

Example 4.3. Convergent representations for many well-known varieties, including the varieties of groups, abelian groups, commutative rings with units, etc. are given in [8]. However, most of them do not satisfy the conditions (*)–(***). Nevertheless, these conditions are satisfied by the representations found in [8] for the varieties of quasigroups, loops, idempotent quasigroups, and unipotent quasigroups. The signature $\mathfrak{F}$ of the representation of the variety of quasigroups, given in [8], consists of three binary operation symbols $\cdot$, $\backslash$ and $/$, and the set of identities is the following:

$$x \cdot (x \backslash y) = y, \tag{4.1}$$

$$(x/y) \cdot y = x, \tag{4.2}$$

$$x \backslash (x \cdot y) = y, \tag{4.3}$$

$$(x \cdot y)/y = x, \tag{4.4}$$

$$(x/y) \backslash x = y, \tag{4.5}$$

$$y/(x \backslash y) = y, \tag{4.6}$$

Adding the identities

$$x \cdot x = x,$$

$$x/x = x,$$

$$x \backslash x = x,$$

we obtain the convergent representation for the variety of idempotent quasigroups.

Similarly, adding one constant 1 to the signature and the identities

$$1 \cdot x = x$$

$$x \cdot 1 = x,$$

$$x/1 = x,$$

$$x \backslash x = 1,$$

$$x/x = 1,$$

$$1 \backslash x = x,$$

to the system (4.1)-(4.6), one obtains the convergent representation for the variety of loops.

Recall that a quasigroup is called unipotent if $x^2 = y^2$ for all elements x, y of the quasigroup. Adding one constant 1 to the signature $\mathfrak{F} = \{\cdot, \backslash, /\}$ and the identities

$$x \cdot x = 1,$$

$$1/x = x,$$

$$x \backslash 1 = x,$$

to the system (4.1)-(4.6), one obtains the convergent representation of the variety of unipotent quasigroups.

Example 4.4. One can easily verify that the following systems are confluent.
(i) Let $\mathfrak{F}$ consist of one binary operation symbol $\cdot$ and Σ consist of the identities

$$x \cdot x = x,$$

$$x \cdot (x \cdot y) = x \cdot y,$$

$$(x \cdot y) \cdot y = x \cdot y.$$

(ii) Let $\mathfrak{F}$ consist of two binary operation symbols $+$ and $\cdot$, one constant, and Σ consist of the identities:

$$x \cdot x = 0,$$

$$x \cdot (x + y) = x \cdot y,$$

$$x + 0 = x,$$

$$0 + x = x,$$

$$x \cdot 0 = 0,$$

$$0 \cdot x = 0.$$

(iii) Let $\mathfrak{F}$ consist of one binary operation symbol $\cdot$, one constant 1, and Σ consist of the identities

$$x \cdot x = 1; \tag{4.7}$$

$$1 \cdot x = 1 \tag{4.8}$$

$$x \cdot 1 = x; \tag{4.9}$$

$$x \cdot (x \cdot y) = y. \tag{4.10}$$

These identities determine the variety of left Steiner loops. Similarly, the system of identities (4.7)-(4.9) together with

$$(x \cdot y) \cdot y = x \tag{4.11}$$

determines the variety of right Steiner loops. Both systems are confluent.

Observe that the system of all identities (4.7)-(4.11) defining the variety of Steiner loops is not confluent. Indeed, overlapping the identity (4.10) with the renamed copy of (4.11) at the position (22), we obtain the non-joinable critical pair $(f(f(s, z), s), s)$ (the symbol f is used here for the binary operation). In order to make it joinable, we need to add the identity $f(f(s, z), s) = s$ to the list of axioms. But then, overlapping the identity (4.11) with the latter one at the position (21), we obtain the non-joinable critical pair $(f(z, s), f(s, z))$. The corresponding identity can not be added to the list of axioms since otherwise the condition (*) would fail.

5   Effective codescent morphisms

Recall the following definition. Let $p : B \to E$ be a morphism in a category $\mathcal{C}$ with pushouts. It is well known that the change-of-cobase functor

$$p_* : B/\mathcal{C} \longrightarrow E/\mathcal{C}$$

(pushing out along p) has a right adjoint $p^!$ composing with p from the right. p is called a *codescent* (resp. *effective codescent*) *morphism* if p_* is precomonadic (resp. comonadic), i.e., the comparison functor

$$\Phi_p : B/\mathcal{C} \longrightarrow \mathbf{Codes}(p),$$

where $\mathbf{Codes}(p)$ is the Eilenberg-Moore category of the comonad induced by the adjunction

$$p_* \dashv p^!,$$

is full and faithful (resp. an equivalence of categories) [11].

One can easily verify that Theorem 4.3 of [21] remains valid in the context of the present paper. Namely we have

Theorem 5.1. Let $\mathcal{C}$ be the variety of universal algebras given with a representation $(\mathfrak{F}, \Sigma)$ which satisfies the condition (*) and which has unique normal forms for the elements of amalgamated free products. Then all codescent morphisms of $\mathcal{C}$ are effective.

From Theorems 3.8 and 5.1 we obtain

Theorem 5.2. Let a variety $\mathcal{C}$ be represented with a confluent term rewriting system $(\mathfrak{F}, \Sigma)$ satisfying the conditions (*)-(***). Then every codescent morphism of $\mathcal{C}$ is effective.

Corollary 5.3. Every codescent morphism is effective in all varieties given in Example 2.9 and Examples 4.1 -4.4. In particular, this is the case for the variety of Mal'tsev algebras, and the varieties of magmas with unit and two-sided inverses, left Steiner loops, right Steiner loops, quasigroups, loops, idempotent quasigroups, unipotent quasigroups.

As mentioned in the Introduction, this result for quasigroups and loops has already been obtained in [21].

Corollary 3.9 and Theorem 5.2 naturally give rise to the question whether any variety of universal algebras satisfying the strong amalgamation property has a convergent representation. The answer is negative, the variety of Boolean algebras does not have such a representation [19] in spite the fact that it satisfies the strong amalgamation property [5].

Acknowledgement

References

[1] F. Baader and T. Nipkow, *Term rewriting and all that*, Cambridge University Press, 2006.

[2] L. Bachmair, N. Dershowitz and J. Hsiang, *Orderings for equational proofs*, In 1st IEEE Symp. on Logic in Computer Science, 346-357. IEEE Computer Society Press, 1986.

[3] J. Corbin and M. Bidoit, *A rehabilitation of Robinson's unification algorithm*, In R. Pavon, editor, Information Processing 83, 909-914, North-Holland, 1983.

[4] N. Dershowitz, L. Marcus and A. Tarlecki, *Existence, uniqueness, and construction of rewrite systems*, SIAM J. Computing **17** (1988), 629–639.

[5] Ph. Dwinger and F. M. Yaqub, *Generalized free products of Boolean algebras with an amalgamated subalgebra*, Neder. Akad. Wetensch. Proc. Ser. A 66 = Indag. Math. 25(1963), 225–231.

[6] T. Evans, *On mutiplicative systems defined by generators and relations. I. Normal forms theorems*, Proc. Cambridge Philos. Soc. **47**(1951), 637–649.

[7] J. Gallier, P. Narendran, D. Plaisted, S. Raatz and W. Snyder, *An algorithm for finding canonical sets of ground rewrite rules in polinomial time*, J. ACM **40** (1993), 1–16.

[8] W. Gehrke, *Detailed catalogue of canonical term rewriting systems generated automatically*, Technical report no. 62, Research Institute for Symbolic Computation (RISC), Johannes Lepler University Linz, 1992.

[9] J. Herbrand, *Logical writings*, Reidel, 1971.

[10] G. Huet, *A complete proof of correctness of the Knuth-Bendix completion procedure*, J. Computer and System Sciences, **23** (1981), 11–21,

[11] G. Janelidze and W. Tholen, *Facets of descent, I.* Appl. Categ. Struct. **2** (1994), 1–37.

[12] G. Janelidze and W. Tholen, *Facets of descent, III: monadic descent for rings and algebras.* Appl. Categ. Structures **12(5-6)** (2004), 461–477.

[13] E. W. Kiss, L. Márki, P. Pröhle and W. Tholen, *Categorical algebraic properties. A compendium on amalgamation, congruence extension, epimorphisms, residual smallness and injectivity*, Studia Sci. Math. Hungarica **18** (1983), 79–141.

[14] D. E. Knuth and P.B. Bendix, *Simple word problems in universal algebra*, In. J. Leech, editor, Computational Problems in Abstract Algebra, 263–297, Pergamon Press, 1970.

[15] A. Martelli and U. Montanari, *An efficient unification algorithm*, ACM Trans. Programming Languages and Systems, **4(2)** (1982) 258–282.

[16] B. Mesablishvili, *Pure morphisms of commutative rings are effective descent morphisms for modules – a new proof*, Theory Appl. Categ. **7** (2000), no. 3, 38–42.

[17] M.H.A. Newman, *On theories with a combinatorial definition of "equivalence"*, Annals of Mathematics **43(2)** (1942), 223–243.

[18] M. S. Paterson and M. N. Wegman, *Linear unification*, J. Computer and System Sciences, **16** (1978), 158–167.

[19] R. Socher-Ambrosius, *Boolean algebra admits no convergent term rewriting system*, In R. E. Book, editor, *Proceedings 4th Conference on Rewriting Techniques and Applications, Como (Italy), Lecture Notes in Computer Science* **488** (1991), 264–274.

[20] D. Zangurashvili, *The strong amalgamation property and (effective) codescent morphisms*, Theory Appl. Categ. **11** (2003), n. 20, 438–449.

[21] D. Zangurashvili, *Effective codescent morphisms in some varieties of universal algebras*, Appl. Categ. Struct. **22** (2014), 241–252.