Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE @ DIRECT®
Journal of Symbolic Computation 37 (2004) 343–376

Journal of Symbolic Computation
www.elsevier.com/locate/jsc

Reduction relations for monoid semirings

Friedrich Otto[a,*], Olga Sokratova[b,1]

[a] *Fachbereich Mathematik/Informatik, Universität Kassel, 34109 Kassel, Germany*
[b] *Institute of Computer Science, University of Tartu, Liivi 2, 50409 Tartu, Estonia*

Received 3 May 2002; accepted 2 July 2003

Abstract

In this paper we study rewriting techniques for monoid semirings. Based on disjoint and non-disjoint representations of the elements of monoid semirings we define two different reduction relations. We prove that in both cases the reduction relation describes the congruence that is induced by the underlying set of equations, and we study the termination and confluence properties of the reduction relations.

Keywords: Semiring; Congruence; Rewriting system; Reduction relation; Termination; Confluence; Critical pair

1. Introduction

Introduced originally by Axel Thue as a method for solving word problems, rewriting theory has become a powerful tool in symbolic computation. We refer to Baader and Nipkow (1998) and Book and Otto (1993) for background concepts and recent results on rewriting systems.

On the other hand, semirings have been found useful for solving problems in different areas of applied mathematics and theoretical computer science. Recently, semirings have been applied in graph theory, optimization, coding theory, automata theory, descriptions of relational data bases, formal language theory, and the study of parallel computational systems (see, e.g., DasGupta and Sontag, 2001; Golan, 1999; Hebisch and Weinert, 1998). Each semiring can be presented as a factor-semiring of a certain polynomial semiring

[*] Corresponding author. Tel.: +49-561-804-4573; fax: +49-561-804-4008.
E-mail addresses: otto@theory.informatik.uni-kassel.de (F. Otto), osokrato@math.uiowa.edu, olga@cs.ut.ee (O. Sokratova).

[1] Currently visiting the Computer Science Department, The University of Iowa, Iowa City, IA 52242-1419, USA.

0747-7171/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2003.07.002

modulo a congruence. In these settings one is interested in congruences on the monoid semirings that are induced by finite sets of equations (Mal'cev, 1954; Sokratova, 2001).

In Mora (1985) it is shown how string rewriting can be applied to monoid rings, in this way extending Gröbner basis computations from commutative rings to certain non-commutative rings. Actually, if R is a ring and X^* denotes the free monoid over a set X of free generators, then a string rewriting system $T \subset X^* \times X^*$ yields a reduction relation $\longrightarrow_T$ on the free monoid X^* as well as a reduction relation $\Longrightarrow_T$ on the free monoid ring RX^*. In fact, if $u, v \in X^*$ are two strings, then u and v are congruent with respect to the Thue congruence $\longleftrightarrow_T^*$ on X^* that is induced by $\longrightarrow_T$, if and only if the polynomial $u - v$ belongs to the two-sided ideal of RX^* that is generated by the set of polynomials $\{u_i - v_i \mid (u_i, v_i) \in T\}$. Thus, string rewriting techniques can be applied to free monoid rings. It turned out that this approach works quite well in those cases, where the underlying monoids are presented by finite convergent string rewriting systems of certain restricted forms (Madlener and Reinert, 1998a,b).

Now the question arises of whether this approach can be extended to monoid semirings. However, there are various problems that must be overcome.

Any congruence relation ρ on a ring is uniquely defined by an ideal I that is the zero class of ρ. More precisely, two elements a and b are congruent with respect to ρ if and only if their difference $a - b$ belongs to I. This allows us to turn any element of an ideal into a rewriting rule.

The zero class of a congruence in a semiring, however, though being an ideal, does in general not uniquely determine a congruence. Thus, in semirings we have to deal with relations, not ideals. For example, the Thue congruence $\longleftrightarrow_T^*$ on X^* translates into the congruence on the semiring RX^* that is generated by the same set T.

The question arises now of how to extend this to an arbitrary finitely generated congruence on RX^*. That is, how to define a reduction relation on RX^* that is based on a (finite) set of polynomials and that represents a given congruence?

Here we undertake a first step into the direction of carrying (string) rewriting techniques over to monoid semirings. If

$$(p, q) := (r_1u_1 + r_2u_2 + \cdots + r_mu_m, s_1v_1 + s_2v_2 + \cdots + s_nv_n)$$

is a pair of polynomials from the free monoid semiring RX^*, where $r_i, s_j \in R \setminus \{0\}$ and $u_i, v_j \in X^*$, and if $\succeq$ is a term ordering on X^*, then there is a unique term, say u_1, that is larger than all other terms u_i, v_j with respect to $\succeq$. Now, if R is actually a ring, that is, it admits the operation of subtraction, then we can replace the pair (p, q) by the pair

$$(r_1u_1, s_1v_1 + s_2v_2 + \cdots + s_nv_n - r_2u_2 - \cdots - r_mu_m),$$

and we can then define a reduction relation that is based on (finite) sets of rules of this particular form.

In this paper we will restrict ourselves to congruences on semirings that are generated by pairs of polynomials of the form above. It appears that in this setting, we can define reduction relations. Actually, we define and study two possible kinds of reduction relations on monoid semirings. The important properties of the reduction relations that we are interested in are local confluence, confluence, and termination. The reduction relations we consider are natural extensions of string rewriting relations. This makes it possible to use string rewriting techniques also in the semiring setting. In particular, we are interested in the connection between the (string) reduction relation on a free monoid and the induced reduction relation on a corresponding monoid semiring.

The two reduction relations studied in this paper are based on different representations of the elements of the monoid semirings considered. For the first reduction relation, called *weak reduction*, we consider a relation $T \subset M \times RM$ in Section 3, where R is a semiring and M is a monoid. We present an element of the monoid semiring RM simply as a finite sum of monomials, where several monomials containing the same term (that is, monoid element) are allowed. A reduction $\Longrightarrow_T$ replaces one of these monomials by a polynomial. This relation is compatible with the operations of addition and multiplication on RM, and it captures the semiring congruence on RM that is generated by T. Hence, the weak reduction is very natural and easy to work with. Unfortunately, it is not terminating in many cases, e.g., if the underlying semiring R is actually a ring, or if R contains idempotents with respect to addition (see Section 3).

Therefore, we study the weak reduction in detail only for the special case of free monoid semirings over the semiring of natural numbers $\mathbb{N}$, that is, $R = \mathbb{N}$ and M is a free monoid X^* over some set X of free generators. As $\mathbb{N}$ is the most natural example of a semiring that is not a ring, $\mathbb{N}X^*$ is probably the most basic form of a monoid semiring. For this particular case we will see that the weak reduction relation terminates, if it is compatible with a suitably chosen admissible well-founded partial ordering on X^*. Next, we study the weak reduction relation for the special case that the underlying set T of rules (or equations) is a string rewriting system $T \subset X^* \times X^*$, and we show that in this case the properties of termination, local confluence, and confluence on $\mathbb{N}X^*$ are inherited from the string rewriting relation $\longrightarrow_T$ on the free monoid X^*. Finally, we present a test for (local) confluence for the weak reduction relation on $\mathbb{N}X^*$ for the more general case that T is a finite relation of the form $T \subset X^* \times \mathbb{N}X^*$. Unfortunately this test, which is based on the notion of critical pair, does not apply to systems that have coefficients larger than 1 on their left-hand sides.

In order to get around the aforementioned termination problem we consider a more restricted reduction relation in Section 4. This relation, called *strong reduction*, is based on the representation of the elements of the monoid semiring RX^* considered as a disjoint sum, that is, if $p = r_1u_1 + r_2u_2 + \cdots + r_nu_n$ ($r_i \in R \setminus \{0\}$, $u_i \in X^*$), then it is required that the monoid elements u_i are pairwise distinct. We concentrate again on the case that $T \subset X^* \times RX^*$, and a reduction step $p \Longrightarrow_T q$ now replaces exactly one of the distinct monomials of p by a corresponding polynomial. As for a disjoint sum of the form above the weak reduction $\Longrightarrow_T$ coincides with the strong reduction $\Longrightarrow_T$, we see that the difference between the two relations simply consists in the requirement that before the strong reduction can be applied the polynomial considered is brought into the form of a disjoint sum by applying the laws of associativity and commutativity of addition in RX^*. Hence, the strong reduction relation can be interpreted as using the weak reduction relation modulo associativity and commutativity of addition.

We will see that the strong reduction relation $\Longrightarrow_T$ generates the smallest congruence on RX^* containing T. We prove that this reduction relation terminates if it is compatible with an admissible well-founded partial ordering on the free monoid X^*. Then we consider the special case of a string rewriting system $T \subset X^* \times X^*$, and we will see that again termination and confluence are inherited from the free monoid. Finally, in Section 4.3 we present a test for (local) confluence of the strong reduction relation on RX^* that is defined by a finite relation $T \subset X^* \times RX^*$ for the case where the semiring R is commutative with respect to multiplication. However, in contrast to the situation for weak reduction, the confluence test for the strong reduction relation requires that this reduction relation is terminating.

Finally, we describe in short the structure of normal forms with respect to a convergent, that is, terminating and confluent, reduction system on a monoid semiring RX^*, and we address the choice of a reduction strategy to compute the normal form of a given element. The paper ends with a short discussion of the problems one is faced with when trying to develop a Knuth–Bendix style completion procedure for free monoid semirings.

2. Preliminaries

Throughout the paper we use the following definitions.

Definition 2.1. A *semiring* $(R, +, \cdot, 0, 1)$ is defined to be a non-empty set R with binary operations of addition $+$ and multiplication $\cdot$ such that $(R, +)$ is a commutative monoid with neutral element 0, $(R, \cdot)$ is a monoid with identity 1, multiplication distributes over addition from either side, and $0 \cdot r = r \cdot 0 = 0$ for all $r \in R$.

Example 2.2. Any ring is a semiring.

Example 2.3. The set $\mathbb{N}$ of non-negative integers with the usual operations of addition and multiplication is a semiring.

The next example provides semirings that are idempotent with respect to addition.

Example 2.4. *Exotic* semirings are certain subsets of $\mathbb{R}$ equipped with the binary operations of minimum or maximum as sum, and addition as product. Two prime examples of such structures are the (max, +)-semiring

$$(\mathbb{R} \cup \{-\infty\}, \max, +, -\infty, 0)$$

and the *tropical* semiring

$$(\mathbb{N} \cup \{\infty\}, \min, +, \infty, 0)$$

(see e.g., Pin, 1998).

The definition of the monoid semiring is similar to that of a monoid ring.

Definition 2.5. For a monoid M, the *monoid semiring* RM consists of all finite sums of the form $\sum_{i=1}^{n} r_i u_i$, where $r_i \in R$, $u_i \in M$, with addition and multiplication defined by the rules

$$\sum_{i=1}^{n} r_i u_i + \sum_{i=1}^{n} r_i' u_i = \sum_{i=1}^{n} (r_i + r_i') u_i,$$

$$\left(\sum_{i=1}^{n} r_i u_i\right) \left(\sum_{j=1}^{n} r_j' u_j\right) = \sum_{i,j=1}^{n} (r_i r_j') u_i u_j.$$

In particular, given a set X, the free monoid semiring RX^* consists of all polynomials over R in the non-commuting variables X.

We will use the representation $p = r_1u_1 \dot{+} \cdots \dot{+} r_nu_n$ for the elements of RM in order to emphasize that all u_i in p are pairwise distinct. Accordingly we call such a representation a *disjoint sum*. In this case r_i is called the *coefficient* of u_i in p. We will denote the coefficient of a monomial u in p by $\pi_p(u)$. For a polynomial $p = r_1u_1 \dot{+} \cdots \dot{+} r_nu_n$, let $\mathrm{TERM}(p) = \{u_1, \ldots, u_n\}$ be the set of *terms* of p.

Definition 2.6. For a set of pairs $T \subset RM \times RM$, $\Theta(T)$ denotes the *congruence* of RM that is generated by T. That is, $\Theta(T)$ is the smallest equivalence relation on RM that contains T, and that is closed under addition and multiplication from the left and from the right.

It is congruences of RM of the form $\Theta(T)$ that we want to study. For doing so we introduce two kinds of reduction relations in the following two sections.

3. Weak reductions for monoid semirings

Let R be a semiring, let M be a monoid, and let RM denote the monoid semiring of M over R.

Definition 3.1. Let $T \subset M \times RM$ be a relation, and let $a, b \in RM$. We define the (*single-step*) *reduction relation* $\Longrightarrow_T$ on RM as follows:

$$\begin{aligned} a \Longrightarrow_T b \qquad & \text{iff } \exists r, r_i \in R \smallsetminus \{0\}\, \exists u, v, u_i \in M\, \exists (x, z) \in T: \\ & a = ruxv + r_1u_1 + \cdots + r_ku_k, \qquad \text{and} \\ & b = ruzv + r_1u_1 + \cdots + r_ku_k. \end{aligned} \tag{1}$$

The relation $\Longrightarrow_T$ is the *weak reduction relation* that is induced by T. It is called *weak* to contrast it with the *strong* reduction relation that will be defined in the next section. If $a = ruxv \dot{+} r_1u_1 \dot{+} \cdots \dot{+} r_ku_k$ is a disjoint sum, and if $r = r_0 + r'$ for some elements $r_0, r' \in R$, $r_0 \neq 0$, then

$$a \Longrightarrow_T r_0uzv + r'uxv + r_1u_1 + \cdots + r_ku_k,$$

that is, the monomial $ruxv$ of a may be replaced only partially by this reduction step. The reflexive transitive closure of $\Longrightarrow_T$ is denoted by $\overset{*}{\Longrightarrow}_T$, its symmetric closure is $\Longleftrightarrow_T$, and the equivalence relation on RM generated by $\Longrightarrow_T$ is denoted by $\overset{*}{\Longleftrightarrow}_T$.

Our first lemma states that the relation $\overset{*}{\Longrightarrow}_T$ is compatible with the operations of addition and multiplication of RM.

Lemma 3.2. *Let $T \subset M \times RM$. For all $a, b, c \in RM$, if $a \overset{*}{\Longrightarrow}_T b$, then $a + c \overset{*}{\Longrightarrow}_T b + c$, $ac \overset{*}{\Longrightarrow}_T bc$, and $ca \overset{*}{\Longrightarrow}_T cb$.*

Proof. Let a and b be elements of RM such that $a \Longrightarrow_T b$. We may assume that a and b are written as in (1). Then it is obvious that

$$\begin{aligned} a + c &= ruxv + r_1u_1 + \cdots + r_ku_k + c \\ &\Longrightarrow_T ruzv + r_1u_1 + \cdots + r_ku_k + c = b + c \end{aligned}$$

holds. Thus, $\Longrightarrow_T$ and $\overset{*}{\Longrightarrow}_T$ are compatible with addition.

Next let $s \in R$ and $w \in M$, and $c := sw$. Then

$$ac = (rs)uxvw + (r_1s)u_1w + \cdots + (r_ks)u_kw,$$

and

$$bc = (rs)uzvw + (r_1s)u_1w + \cdots + (r_ks)u_kw.$$

If $rs = 0$, then $ac = bc$, otherwise $ac \Longrightarrow_T bc$. Finally, if

$$c = s_1w_1 + \cdots + s_mw_m,$$

then

$$\begin{aligned} ac \quad &= \quad as_1w_1 + as_2w_2 + \cdots + as_mw_m \\ &\overset{*}{\Longrightarrow}_T bs_1w_1 + as_2w_2 + \cdots + as_mw_m \\ &\overset{*}{\Longrightarrow}_T bs_1w_1 + bs_2w_2 + \cdots + as_mw_m \\ &\overset{*}{\Longrightarrow}_T \cdots \\ &\overset{*}{\Longrightarrow}_T bs_1w_1 + \cdots + bs_mw_m = bc. \end{aligned}$$

Hence, $\overset{*}{\Longrightarrow}_T$ is compatible with multiplication from the right, and by symmetry it follows that it is also compatible with multiplication from the left. □

Next we will see that the reduction relation $\Longrightarrow_T$ captures the congruence $\Theta(T)$ on RM that is generated by T.

Theorem 3.3. *Let $T \subset M \times RM$. Then $\overset{*}{\Longleftrightarrow}_T = \Theta(T)$.*

Proof. First, we verify that $\overset{*}{\Longleftrightarrow}_T$ is a congruence on RM. Obviously, it is an equivalence relation. Further, it satisfies the substitution property, that is, it is compatible with addition and multiplication, as the reduction relation $\overset{*}{\Longrightarrow}_T$ is (Lemma 3.2). Thus, $\overset{*}{\Longleftrightarrow}_T$ is indeed a congruence relation on RM. Since $T \subset \overset{*}{\Longleftrightarrow}_T$, it follows that $\Theta(T) \subseteq \overset{*}{\Longleftrightarrow}_T$.

To prove that $\overset{*}{\Longleftrightarrow}_T$ is contained in $\Theta(T)$, we take any pair (a, b) with $a \Longrightarrow_T b$. Since $\Theta(T)$ is a congruence, the definition (1) implies that $(a, b) \in \Theta(T)$. Since $\Theta(T)$ is an equivalence relation, it follows that $\overset{*}{\Longleftrightarrow}_T \subseteq \Theta(T)$. Hence, we see that $\overset{*}{\Longleftrightarrow}_T = \Theta(T)$, as required. □

Unfortunately, the reduction relation $\Longrightarrow_T$ defined by (1) does not seem to be an appropriate tool for many monoid semirings. This is illustrated by the following examples.

Example 3.4. Let $R := \mathbb{Z}$, let $X := \{x, y\}$, let M be the free monoid X^*, and let $T := \{(x, y)\}$. On M the system T generates the string rewriting relation $\longrightarrow_T$, which is defined by $uxv \longrightarrow_T uyv$ for all $u, v \in M$. Obviously, this relation is terminating, that is, there is no infinite sequence of the form

$$w_0 \longrightarrow_T w_1 \longrightarrow_T \cdots \longrightarrow_T w_i \longrightarrow_T w_{i+1} \longrightarrow_T \cdots$$

in M. However, for the reduction relation $\Longrightarrow_T$ the situation is totally different, as

$$y = y + x - x \Longrightarrow_T y + x - y = x \Longrightarrow_T y.$$

Thus, this relation is not terminating.

The problem with termination in Example 3.4 stems from the fact that the underlying semiring is actually a ring, that is, it provides inverse elements with respect to addition. The next example shows that the same problem arises when the semiring contains idempotent elements with respect to addition (cf. Example 2.4).

Example 3.5. Let R be a semiring with an element $r \in R \setminus \{0\}$ that is idempotent with respect to addition, that is, $r + r = r$, let $X := \{x, y\}$, $M := X^*$, and $T := \{(x, y)\}$. Then

$$\begin{aligned} rx + ry &= (r + r)x + ry = rx + rx + ry \Longrightarrow_T rx + ry + ry \\ &= rx + (r + r)y = rx + ry, \end{aligned}$$

which shows that also in this case $\Longrightarrow_T$ is not terminating.

Therefore we investigate this reduction relation only for the special case of free monoid semirings over the natural numbers.

3.1. *The reduction relation $\Longrightarrow_T$ for free monoid semirings over $\mathbb{N}$*

For the rest of this section we only consider the semiring $\mathbb{N}$ of natural numbers, and free monoid semirings of the form $\mathbb{N}X^*$.

Definition 3.6. We define the set of monomials ${}_{\mathbb{N}}X^*$ as

$${}_{\mathbb{N}}X^* := \{nu \mid n \in \mathbb{N} \setminus \{0\}, u \in X^*\}.$$

Due to the possibility of performing division in $\mathbb{N}X^*$, we are able to consider slightly more general relations as before.

Definition 3.7. Let $T \subset {}_{\mathbb{N}}X^* \times \mathbb{N}X^*$, and let $a, b \in \mathbb{N}X^*$.

For a relation of this form the reduction relation $\Longrightarrow_T$ is defined as follows:

$$\begin{aligned} a \Longrightarrow_T b \qquad &\text{iff } \exists r, r_i \in \mathbb{N} \setminus \{0\}\, \exists u, v, u_i \in X^*\, \exists (nx, z) \in T: \\ &a = (r \cdot n)uxv + r_1u_1 + \cdots + r_ku_k, \qquad \text{and} \\ &b = ruzv + r_1u_1 + \cdots + r_ku_k. \end{aligned} \tag{2}$$

Thus, here we consider relations T for which the left-hand side of an element of T may have a coefficient larger than 1. It is easily seen that the relation $\overset{*}{\Longrightarrow}_T$ is compatible with addition and multiplication, and that it satisfies Theorem 3.3, too. In this particular setting termination is guaranteed by the following technical result.

Recall that a partial ordering $\succeq$ on X^* is called *admissible* if, for all u, v, x, y in X^*, $u \succeq v$ implies $xuy \succeq xvy$. A partial ordering $\succeq$ on X^* is called *well-founded* if no infinite chains of the form $u_1 \succ u_2 \succ \cdots$ with $u_i \in X^*$ exist, where $\succ$ denotes the proper part of $\succeq$, that is, $u \succ v$ holds if $u \succeq v$ and $u \neq v$.

Theorem 3.8. *Let $\succeq$ be an admissible well-founded partial ordering on X^*, and let $T \subset {}_{\mathbb{N}}X^* \times \mathbb{N}X^*$ be a relation on $\mathbb{N}X^*$ such that the following conditions are satisfied for each pair $(ru, s_1v_1 \dotplus \cdots \dotplus s_nv_n)$ of T:*

- *$u \succeq v_i$, for all $i = 1, \ldots, n$, and*
- *$r > s_i$, whenever $u = v_i$.*

Then $\Longrightarrow_T$ is terminating.

Proof. Notice that every polynomial $r_1u_1 \dotplus \cdots \dotplus r_nu_n$ of $\mathbb{N}X^*$ can be interpreted as a multiset over X^* containing r_i copies of u_i. The well-founded partial ordering $\succeq$ on X^* induces a well-founded partial ordering $\underline{\succ\!\succ}$ on the set of multisets over X^* (see Dershowitz and Manna, 1979). This multiset ordering then gives a well-founded partial ordering $\underline{\succ\!\succ}$ on $\mathbb{N}X^*$. This ordering compares two polynomials

$$p = r_1u_1 \dotplus \cdots \dotplus r_nu_n$$

and

$$q = r_1'u_1 \dotplus \cdots \dotplus r_n'u_n \dotplus s_1v_1 \dotplus \cdots \dotplus s_mv_m \neq p$$

as follows:

$$p \succ\!\succ q$$

iff

$$\forall i \in \{1, \ldots, m\}\, \exists j \in \{1, \ldots, n\}\colon u_j \succ v_i \text{ and } r_j > r_j', \text{ and}$$
$$\forall i \in \{1, \ldots, n\}\colon (r_i \geq r_i' \text{ or } \exists j \in \{1, \ldots, n\}\colon u_j \succ u_i \text{ and } r_j > r_j').$$

It is easily seen that $\underline{\succ\!\succ}$ is *compatible* with $\Longrightarrow_T$, that is, $p \Longrightarrow_T p'$ implies $p \succ\!\succ p'$. Hence, $\Longrightarrow_T$ is terminating. □

3.2. Restricted reduction systems

We are concerned with the properties of the reduction relation $\Longrightarrow_T$ that is induced by a finite relation $T \subset {}_{\mathbb{N}}X^* \times \mathbb{N}X^*$. Theorem 3.8 gives a sufficient condition for establishing termination of $\Longrightarrow_T$. If $\Longrightarrow_T$ is terminating, then each element a of $\mathbb{N}X^*$ has one or more normal forms with respect to $\Longrightarrow_T$, where c is called a *normal form* of a if $a \overset{*}{\Longrightarrow}_T c$ and c is *irreducible* mod $\Longrightarrow_T$, that is, $c \Longrightarrow_T d$ does not hold for any $d \in \mathbb{N}X^*$. If, in addition to being terminating, $\Longrightarrow_T$ is confluent, then each a has a unique normal form. Hence, we would like to characterize those relations T for which $\Longrightarrow_T$ is confluent.

We start this investigation by considering the special case where T is a string rewriting system on X^*, that is, $T \subset X^* \times X^*$. Then the system T induces two reduction relations:

the reduction relation $\xrightarrow{*}_T$ on X^* that is defined by

$$\begin{aligned} u \longrightarrow_T v \qquad & \text{iff } \exists x, y \in X^* \, \exists (w, w') \in T: \\ & u = xwy \qquad \text{and} \qquad v = xw'y, \end{aligned} \tag{3}$$

and the reduction relation $\Longrightarrow_T$ on $\mathbb{N}X^*$ that is defined by (2).

It is an immediate consequence of these definitions that the relation $\Longrightarrow_T$ can simply be interpreted as an extension of the relation $\longrightarrow_T$. This is made precise by the following proposition.

Proposition 3.9. *Let (X, T) be a string rewriting system. Then the following conditions are equivalent for all strings $u, v \in X^*$:*

(a) *$u \longrightarrow_T v$ in X^*,*

(b) *$u \Longrightarrow_T v$ in $\mathbb{N}X^*$.*

Under what conditions does the relation $\Longrightarrow_T$ inherit properties such as termination, local confluence, or confluence from the relation $\longrightarrow_T$? In the following we will address this question. Our first result deals with the termination property.

Proposition 3.10. *Let (X, T) be a finite string rewriting system. Then the reduction relation $\Longrightarrow_T$ on $\mathbb{N}X^*$ is terminating iff $\longrightarrow_T$ is terminating.*

Proof. If $\Longrightarrow_T$ is terminating, then by Proposition 3.9 also $\longrightarrow_T$ is terminating. Conversely, assume that $\longrightarrow_T$ is terminating. We obtain a partial ordering $\succeq$ on X^* by defining its proper part $\succ$ as follows:

$$u \succ v \qquad \text{iff } u \xrightarrow{+}_T v.$$

Then $\succeq$ is an admissible partial ordering that is well-founded. Also $u \succ v$ holds for each rule $(u, v) \in T$. Hence, Theorem 3.8 yields that $\Longrightarrow_T$ is terminating on $\mathbb{N}X^*$. □

An analogous result holds for local confluence.

Theorem 3.11. *Let (X, T) be a finite string rewriting system. Then the reduction relation $\Longrightarrow_T$ on $\mathbb{N}X^*$ is locally confluent iff $\longrightarrow_T$ is locally confluent.*

Proof. The ‘only if’ part is obvious by Proposition 3.9.

To prove the ‘if’ part we take three elements $a, b, c \in \mathbb{N}X^*$ such that $a \Longrightarrow_T b$ and $a \Longrightarrow_T c$. Let a have the following representation as a disjoint sum:

$$a = r_1 u_1 \dot{+} \cdots \dot{+} r_k u_k.$$

It follows that there exist indices i and j, natural numbers $r_i' \leq r_i$, $r_j'' \leq r_j$, and strings $u_i', u_j'' \in X^*$ such that $u_i \longrightarrow_T u_i'$, $u_j \longrightarrow_T u_j''$, and

$$\begin{aligned} b &= r_1 u_1 + \cdots + (r_i - r_i')u_i + r_i' u_i' + \cdots + r_k u_k, \\ c &= r_1 u_1 + \cdots + (r_j - r_j'')u_j + r_j'' u_j'' + \cdots + r_k u_k. \end{aligned}$$

First, suppose that $i \neq j$. Then

$$\begin{aligned} b &= r_1u_1 + \cdots + (r_i - r_i')u_i + r_i'u_i' + \cdots + (r_j - r_j'')u_j + r_j''u_j + \cdots + r_ku_k \\ &\Longrightarrow_T r_1u_1 + \cdots + (r_i - r_i')u_i + r_i'u_i' + \cdots + (r_j - r_j'')u_j \\ &\qquad + r_j''u_j'' + \cdots + r_ku_k, \end{aligned}$$

and

$$\begin{aligned} c &= r_1u_1 + \cdots + (r_i - r_i')u_i + r_i'u_i + \cdots + (r_j - r_j'')u_j + r_j''u_j'' + \cdots + r_ku_k \\ &\Longrightarrow_T r_1u_1 + \cdots + (r_i - r_i')u_i + r_i'u_i' + \cdots + (r_j - r_j'')u_j \\ &\qquad + r_j''u_j'' + \cdots + r_ku_k. \end{aligned}$$

Thus, in this case b and c have a common descendant.

Secondly, suppose that $i = j$. Since $\longrightarrow_T$ is locally confluent, there exists a string $w \in X^*$ such that $u_i' \xrightarrow{*}_T w$ and $u_j'' = u_i'' \xrightarrow{*}_T w$. We have

$$\begin{aligned} b &= r_1u_1 + \cdots + (r_i - r_i')u_i + r_i'u_i' + \cdots + r_ku_k \\ &\overset{*}{\Longrightarrow}_T r_1u_1 + \cdots + (r_i - r_i')u_i' + r_i'u_i' + \cdots + r_ku_k \\ &= r_1u_1 + \cdots + r_iu_i' + \cdots + r_ku_k \\ &\overset{*}{\Longrightarrow}_T r_1u_1 + \cdots + r_iw + \cdots + r_ku_k \end{aligned}$$

and

$$\begin{aligned} c &= r_1u_1 + \cdots + (r_i - r_i'')u_i + r_i''u_i'' + \cdots + r_ku_k \\ &\overset{*}{\Longrightarrow}_T r_1u_1 + \cdots + (r_i - r_i'')u_i'' + r_i''u_i'' + \cdots + r_ku_k \\ &= r_1u_1 + \cdots + r_iu_i'' + \cdots + r_ku_k \\ &\overset{*}{\Longrightarrow}_T r_1u_1 + \cdots + r_iw + \cdots + r_ku_k. \end{aligned}$$

Thus, also in this case b and c have a common descendant. Hence, $\Longrightarrow_T$ is indeed locally confluent. □

Actually, we can explicitly describe the descendants of a polynomial. For a polynomial

$$a = r_1u_1 \dotplus \cdots \dotplus r_ku_k,$$

any descendant b of a is of the following form:

$$b = \sum_{i=1}^{r_1} u_{1,i} + \cdots + \sum_{i=1}^{r_k} u_{k,i}, \tag{4}$$

where, for $j = 1, \ldots, k$, $u_{j,1}, \ldots, u_{j,r_j}$ are (not necessarily distinct) descendants of u_j. In particular, b is a *normal form* of a if all the strings $u_{j,1}, \ldots, u_{j,r_j}$ are normal forms of u_j mod $\longrightarrow_T$.

Theorem 3.12. *Let (X, T) be a finite string rewriting system. Then $\Longrightarrow_T$ is confluent iff $\longrightarrow_T$ is confluent.*

Proof. The 'only if' part is obvious by Proposition 3.9.

To prove the 'if' part we take three elements $a = r_1u_1 \dotplus \cdots \dotplus r_ku_k$, and b, c such that $a \overset{*}{\Longrightarrow}_T b$ and $a \overset{*}{\Longrightarrow}_T c$. We can write b in the form (4). Since $\longrightarrow_T$ is confluent, we see that, for all $j = 1, \dots, k$, all monomials $u_{j,1}, \dots, u_{j,r_j}$ have a common descendant u'_j. Therefore,

$$b \overset{*}{\Longrightarrow}_T r_1u'_1 + \cdots + r_ku'_k.$$

Similarly,

$$c \overset{*}{\Longrightarrow}_T r_1u''_1 + \cdots + r_ku''_k,$$

where $u_i \xrightarrow{*}_T u''_i$. Since $\longrightarrow_T$ is confluent, there exist $w_i \in X^*$ such that $u'_i \xrightarrow{*}_T w_i$ and $u''_i \xrightarrow{*}_T w_i$. We obtain that $r_1w_1 + \cdots + r_kw_k$ is a common descendant of b and c mod $\Longrightarrow_T$. Thus, $\Longrightarrow_T$ is indeed confluent. □

By combining the above results we obtain the following.

Corollary 3.13. *Let (X, T) be a finite string rewriting system. If $\longrightarrow_T$ is convergent, then $\Longrightarrow_T$ is convergent as well. For $a = r_1u_1 \dotplus \cdots \dotplus r_ku_k$, the unique normal form of a mod $\Longrightarrow_T$ is of the form $r_1\hat{u}_1 + \cdots + r_k\hat{u}_k$, where $\hat{u}_i$ is the unique normal form of the string u_i mod $\longrightarrow_T$. In particular, the congruence $\Theta(T)$ is decidable in $\mathbb{N}X^*$ in this case.*

For actually computing the normal form of $a \in \mathbb{N}X^*$ mod $\Longrightarrow_T$, we propose to use the strong reduction relation $\Rightarrow_T$ that is introduced in Section 4, as it is contained in $\Longrightarrow_T$. On the other hand, in order to prove that two polynomials $a, b \in \mathbb{N}X^*$ are related mod $\Theta(T)$, we may not have to determine and then to compare the normal forms of a and b, but it is enough to show that a and b have a common descendant mod $\Longrightarrow_T$.

Example 3.14. Let $X := \{x, y\}$, and let $T := \{(yx, xy^2)\}$. Then $\longrightarrow_T$ is convergent, and so is $\Longrightarrow_T$. Consider the polynomials $a := 2yx^3$ and $b := yx^3 + xy^2x^2$. Then a and b have the common normal form $c := 2x^3y^8$. The shortest reduction sequence mod $\Longrightarrow_T$ transforming a into c consists of 7 steps, and the shortest sequence transforming b into c has 7 steps as well. However,

$$a = yx^3 + yx^3 \Longrightarrow_T yx^3 + xy^2x^2 = b$$

is a much shorter proof for $(a, b) \in \Theta(T)$.

3.3. *Test for (local) confluence*

If (X, T) is a finite string rewriting system, then by Corollary 3.13 we can use the tools from the theory of string rewriting systems to verify that the reduction relation $\Longrightarrow_T$ on $\mathbb{N}X^*$ is terminating and/or confluent. In particular, if $\longrightarrow_T$ is terminating, then confluence of $\longrightarrow_T$ (and therewith of $\Longrightarrow_T$) is decidable by checking a finite number of critical situations for $\longrightarrow_T$, the so-called *critical pairs*.

Here we will establish a corresponding test for the more general situation of a relation $T \subset {}_{\mathbb{N}}X^* \times \mathbb{N}X^*$. For doing so we first introduce the notions of overlap and of critical pair for $\Longrightarrow_T$.

Let

$$(s_1u_1, r_1v_1 \dotplus r_2v_2 \dotplus \cdots \dotplus r_kv_k) \quad \text{and} \quad (s_2u_2, t_1w_1 \dotplus t_2w_2 \dotplus \cdots \dotplus t_pw_p) \tag{5}$$

be two (not necessarily distinct) rules of T, where $s_1, s_2, r_i, t_j \in \mathbb{N} \setminus \{0\}$ and $u_1, u_2, v_i, w_j \in X^*$.

Definition 3.15. We say that the rules in (5) *overlap* if one of the following two cases holds:

(a) there exist strings $x, y \in X^*$, $0 < |x| < |u_2|$, such that $u_1x = yu_2$;
(b) there exist strings $x, y \in X^*$ such that $u_1 = xu_2y$.

We illustrate this and the following definitions by the following example.

Example 3.16. Let $X := \{x, y, z\}$, and let $T := \{(x^2, y), (yx, xy^2 + xy), (zyx, x + y)\}$. Then T admits four different overlaps:

1. (x^2, y) overlaps with itself, as $x^2 \cdot x = x \cdot x^2$,
2. $(yx, xy^2 + xy)$ overlaps with (x^2, y), as $yx \cdot x = y \cdot x^2$,
3. $(zyx, x + y)$ overlaps with (x^2, y), as $zyx \cdot x = zy \cdot x^2$, and
4. $(zyx, x + y)$ overlaps with $(yx, xy^2 + xy)$, as $zyx = z \cdot yx$.

Here the first three overlaps are obtained by case (a), while the fourth overlap is obtained by case (b) of the above definition.

Let s be the maximum of s_1 and s_2 in (5). If case (a) of Definition 3.15 holds, then both rules of (5) can be applied to the monomial su_1x:

$$su_1x = s_1u_1x + (s - s_1)u_1x \Longrightarrow_T r_1v_1x + r_2v_2x + \cdots + r_kv_kx + (s - s_1)u_1x$$

and

$$su_1x = syu_2 = s_2yu_2 + (s - s_2)yu_2 \Longrightarrow_T t_1yw_1 + \cdots + t_pyw_p + (s - s_2)yu_2.$$

Analogously, if case (b) of Definition 3.15 holds, then both rules are applicable to the monomial su_1:

$$su_1 = s_1u_1 + (s - s_1)u_1 \Longrightarrow_T r_1v_1 + r_2v_2 + \cdots + r_kv_k + (s - s_1)u_1$$

and

$$\begin{aligned} su_1 &= sxu_2y = s_2xu_2y + (s - s_2)xu_2y \\ &\Longrightarrow_T t_1xw_1y + t_2xw_2y + \cdots + t_pxw_py + (s - s_2)xu_2y. \end{aligned}$$

If $\Longrightarrow_T$ is to be (locally) confluent, then in both cases the two immediate descendants of su_1x or of su_1, respectively, need to have a common descendant. Thus, the above situations are of particular interest for checking (local) confluence of $\Longrightarrow_T$. This leads to the following definition.

Definition 3.17. Let $s = \max(s_1, s_2)$. Each overlap of the rules in (5) yields a *critical pair* as follows:
if $u_1x = yu_2$ for some $x, y \in X^*$, $0 < |x| < |u_2|$, then the resulting critical pair is

$$\begin{aligned} &(r_1v_1x + r_2v_2x + \cdots + r_kv_kx + (s - s_1)u_1x, t_1yw_1 + t_2yw_2 \\ &\quad + \cdots + t_pyw_p + (s - s_2)yu_2), \end{aligned}$$

and if $u_1 = xu_2y$ for some $x, y \in X^*$, then the resulting critical pair is

$$(r_1v_1 + r_2v_2 + \cdots + r_kv_k + (s - s_1)u_1, t_1xw_1y + t_2xw_2y \\ + \cdots + t_pxw_py + (s - s_2)xu_2y).$$

By $\mathrm{CP}(T)$ we denote the set of all critical pairs of T.

Example 3.16 (Continued). The overlaps of T result in the following set of critical pairs

$$\mathrm{CP}(T) := \{(yx, xy), (xy^2x + xyx, y^2), (x^2 + yx, zy^2), (x + y, zxy^2 + zxy)\},$$

as

$$\begin{aligned} &y \cdot x \Longleftarrow_T x^2 \cdot x = x \cdot x^2 \Longrightarrow_T x \cdot y, \\ &xy^2 \cdot x + xy \cdot x \Longleftarrow_T yx \cdot x = y \cdot x^2 \Longrightarrow_T y \cdot y, \\ &x \cdot x + y \cdot x \Longleftarrow_T zyx \cdot x = zy \cdot x^2 \Longrightarrow_T zy \cdot y, \\ &x + y \Longleftarrow_T zyx = z \cdot yx \Longrightarrow_T z \cdot xy^2 + z \cdot xy. \end{aligned}$$

For the special case where each element of T has coefficient one on its left-hand side we obtain the following characterization.

Theorem 3.18. *Let $T \subset X^* \times \mathbb{N}X^*$. Then the following statements are equivalent:*

(a) *The relation $\Longrightarrow_T$ is locally confluent.*
(b) *The polynomials p and q have a common descendant* mod $\Longrightarrow_T$ *for each critical pair $(p, q) \in \mathrm{CP}(T)$.*

Proof. Obviously, if $\Longrightarrow_T$ is locally confluent, then all the critical pairs in $\mathrm{CP}(T)$ resolve mod $\Longrightarrow_T$. Thus, it remains to prove the converse implication.

Let a, b, c be three elements of $\mathbb{N}X^*$ such that $a \Longrightarrow_T b$ and $a \Longrightarrow_T c$, where a has the following representation as a direct sum of monomials:

$$a = r_1u_1 \dotplus \cdots \dotplus r_ku_k.$$

We distinguish three cases based on the form of the reduction steps $a \Longrightarrow_T b$ and $a \Longrightarrow_T c$.

Case 1. Let us suppose first that b and c are obtained from a by rewriting at different monomials of a, say at u_1 and at u_2. That is, there exist strings $x_1, x_2, y_1, y_2 \in X^*$, integers $s_1 \le r_1$, $s_2 \le r_2$, and elements $(\ell_1, v), (\ell_2, w) \in T$ such that $u_1 = x_1\ell_1y_1$, $u_2 = x_2\ell_2y_2$, and

$$\begin{aligned} b &= s_1x_1vy_1 + (r_1 - s_1)u_1 + r_2u_2 + \cdots + r_ku_k, \\ c &= r_1u_1 + s_2x_2wy_2 + (r_2 - s_2)u_2 + \cdots + r_ku_k. \end{aligned}$$

Obviously, b and c reduce to a common descendant as follows:

$$\begin{aligned} b &\overset{*}{\Longrightarrow}_T r_1x_1vy_1 + r_2u_2 + \cdots + r_ku_k \\ &\Longrightarrow_T r_1x_1vy_1 + r_2x_2wy_2 + \cdots + r_ku_k, \qquad \text{and} \\ c &\overset{*}{\Longrightarrow}_T r_1u_1 + r_2x_2wy_2 + \cdots + r_ku_k \\ &\Longrightarrow_T r_1x_1vy_1 + r_2x_2wy_2 + \cdots + r_ku_k. \end{aligned}$$

Case 2. If b and c are obtained from a by rewriting at the same monomial, say u_1, then there are two subcases.

Case 2.1. There exist rules (ℓ_1, v) and (ℓ_2, w) in T, strings $x, y, z \in X^*$, and integers $s_1 \leq r_1$ and $s_2 \leq r_1$ such that $u_1 = x\ell_1 y\ell_2 z$ and

$$b = s_1 xvy\ell_2 z + (r_1 - s_1)u_1 + r_2u_2 + \cdots + r_ku_k,$$
$$c = s_2 x\ell_1 ywz + (r_1 - s_2)u_1 + r_2u_2 + \cdots + r_ku_k.$$

As $\overset{*}{\Longrightarrow}_T$ is compatible with addition and multiplication, we see that b and c reduce to a common descendant as follows:

$$\begin{aligned} b &\overset{*}{\Longrightarrow}_T r_1 xvy\ell_2 z + r_2u_2 + \cdots + r_ku_k \\ &\Longrightarrow_T r_1 xvywz + r_2u_2 + \cdots + r_ku_k, \qquad \text{and} \\ c &\overset{*}{\Longrightarrow}_T r_1 x\ell_1 ywz + r_2u_2 + \cdots + r_ku_k \\ &\Longrightarrow_T r_1 xvywz + r_2u_2 + \cdots + r_ku_k. \end{aligned}$$

Case 2.2. The occurrences of ℓ_1 and ℓ_2 in u_1 overlap. Then there exist strings $x, y, z \in X^*$ and a critical pair (p_1, p_2) such that $u_1 = xyz$ and integers $s_1 \leq r_1$ and $s_2 \leq r_1$ such that

$$b = s_1 xp_1 z + (r_1 - s_1)u_1 + r_2u_2 + \cdots + r_ku_k,$$
$$c = s_2 xp_2 z + (r_1 - s_2)u_1 + r_2u_2 + \cdots + r_ku_k.$$

By the hypothesis of the theorem there exists a polynomial q such that p_1 and p_2 both reduce to q mod $\Longrightarrow_T$. Thus, as $\overset{*}{\Longrightarrow}_T$ is compatible with addition and multiplication, we see that b and c reduce to a common descendant as follows:

$$b \overset{*}{\Longrightarrow}_T r_1 xp_1 z + r_2u_2 + \cdots + r_ku_k \overset{*}{\Longrightarrow}_T r_1 xqz + r_2u_2 + \cdots + r_ku_k,$$
$$c \overset{*}{\Longrightarrow}_T r_1 xp_2 z + r_2u_2 + \cdots + r_ku_k \overset{*}{\Longrightarrow}_T r_1 xqz + r_2u_2 + \cdots + r_ku_k.$$

Thus, in each case b and c have a common descendant, implying that $\Longrightarrow_T$ is indeed locally confluent. □

Unfortunately, this characterization does not hold in general for the case that the elements of T have coefficients larger than one on their left-hand sides. This is illustrated by the following example.

Example 3.19. Let $X := \{x, y, z, d, e\}$, and let T consist of the following six 'rules':

(1) $3zx^2y \to zd + 2e$,
(2) $2yx^2 \to 2d$,
(3) $zx^2yx^2 \to 2x + y + z$,
(4) $zdx^2 \to 6x + 3z$,
(5) $2ex^2 \to 3y$,
(6) $zx^2d \to 2x + y + z$.

Using the length-lexicographical ordering on X^*, it is easily seen that $\Longrightarrow_T$ is terminating by Theorem 3.8. Thus, $\Longrightarrow_T$ is confluent if and only if it is locally confluent.

Next we determine the critical pairs of T. For convenience we will label each rewriting step with the number of the rule applied.

(i) The first two rules overlap. The critical pair (p_1, q_1) is obtained by rewriting the monomial $3zx^2yx^2$ with both rules:

$$(3zx^2y)x^2 \Longrightarrow_{(1)} zdx^2 + 2ex^2 =: p_1$$

and

$$3zx^2yx^2 = zx^2yx^2 + zx^2(2yx^2) \Longrightarrow_{(2)} zx^2yx^2 + 2zx^2d =: q_1.$$

As

$$zdx^2 + 2ex^2 \Longrightarrow_{(4)} 6x + 3z + 2ex^2 \Longrightarrow_{(5)} 6x + 3z + 3y$$

and

$$\begin{aligned} zx^2yx^2 + 2zx^2d &\Longrightarrow_{(3)} 2x + y + z + 2zx^2d \\ &\Longrightarrow_{(6)} 2x + y + z + 4x + 2y + 2z = 6x + 3y + 3z, \end{aligned}$$

we see that this critical pair resolves.

(ii) The first rule overlaps with the third rule. The critical pair (p_2, q_2) is obtained by rewriting the monomial $3zx^2yx^2$ with both rules:

$$3zx^2yx^2 \Longrightarrow_{(1)} zdx^2 + 2ex^2 =: p_2$$

and

$$3zx^2yx^2 \Longrightarrow_{(3)} 6x + 3y + 3z =: q_2.$$

As seen above $6x+3y+3z$ is a descendant of $p_2 = p_1$, that is, this pair also resolves.

(iii) The second rule overlaps with the third rule. The critical pair (p_3, q_3) is obtained by rewriting the monomial $2zx^2yx^2$ with both rules:

$$2zx^2yx^2 = zx^2(2yx^2) \Longrightarrow_{(2)} 2zx^2d =: p_3$$

and

$$2zx^2yx^2 \Longrightarrow_{(3)} 4x + 2y + 2z =: q_3.$$

As

$$p_3 = 2zx^2d \Longrightarrow_{(6)} 4x + 2y + 2z = q_3,$$

this pair also resolves.

These are all the critical pairs of T. However, consider the following reductions corresponding to Case 2.1 in the above proof:

$$(3zx^2y)ex^2 \Longrightarrow_{(1)} zdex^2 + 2e^2x^2 \Longrightarrow_{(5)} zdex^2 + 3ey,$$

which is irreducible mod $\Longrightarrow_T$, and

$$\begin{aligned} 3zx^2yex^2 &= zx^2yex^2 + zx^2y(2ex^2) \Longrightarrow_{(5)} zx^2yex^2 + 3zx^2y^2 \\ &\Longrightarrow_{(1)} zx^2yex^2 + zdy + 2ey, \end{aligned}$$

which is also irreducible mod $\Longrightarrow_T$. Thus, $\Longrightarrow_T$ is not (locally) confluent.

The problem stems from the following fact. If the left-hand side of each element of T has coefficient one, then, for each $n \geq 1$ and each $u \in X^*$, if $n \cdot u$ is reducible mod $=\!=\!\!>_T$, then so is $m \cdot u$ for each $m \geq 1$. However, if the left-hand sides of some elements of T have coefficients of size larger than one, this is not true anymore, as seen in the example above. Thus, for this situation we would need a much more general definition of overlaps and critical pairs that also takes the coefficients into account.

4. Reductions that are based on disjoint sums

Here we return to the case of free monoid semirings RX^*, where R is an arbitrary semiring and X^* is a free monoid.

As the reduction relation $\overset{*}{=\!=\!\!>}_T$ is in general non-terminating, we consider a more restricted reduction relation. This reduction relation is based on representations of elements of the monoid semiring considered as a disjoint sum of monomials as defined in Section 2.

Definition 4.1. Let $T \subset X^* \times RX^*$ be a relation such that, for every pair $(w, w') \in T$, the string w does not appear in $\text{TERM}(w')$. We define a *one-step reduction relation* $\Longrightarrow_T$ on RX^* as follows:

$$\begin{aligned} &a \Longrightarrow_T b \qquad \text{iff } \exists r, r_i \in R \smallsetminus \{0\}\, \exists u, v, u_i \in X^*\, \exists (w, w') \in T: \\ &a = ruwv \dotplus r_1u_1 \dotplus \cdots \dotplus r_ku_k, \\ &b = ruw'v + (r_1u_1 \dotplus \cdots \dotplus r_ku_k). \end{aligned} \tag{6}$$

As the polynomial $ruw'v$ may contain one or more of the terms $u_1, \ldots, u_k$, the given representation of the element b is in general not a disjoint sum. Since, in contrast to $=\!=\!\!>_T$, a monomial is rewritten completely in each $\Longrightarrow_T$-step, we call $\Longrightarrow_T$ the *strong reduction relation* that is induced by T.

In Lemma 3.2 we have seen that the weak reduction relation is compatible with addition and multiplication. This is not true for the strong reduction relation, however, as shown by the following example.

Example 4.2. Let $R := \mathbb{N}$, $X := \{x, y\}$, and $T := \{(x^2, y)\}$. Consider the polynomials $a := x^2$, $b := y$, and $c := x^2$. Then $a \Longrightarrow_T b$, but $a + c = 2x^2$ does not reduce to $b + c = y + x^2$ mod $\Longrightarrow_T$. Thus, $\Longrightarrow_T$ is in general not compatible with addition.

The following lemma shows that the strong reduction relation is at least compatible with multiplication by monomials from the left and from the right.

Lemma 4.3. *Let $a, b \in RX^*$, and let $r, r' \in R$ and $w, w' \in X^*$.*

(a) *If $a \Longrightarrow_T b$, then $rw \cdot a \cdot r'w' \Longrightarrow_T rw \cdot b \cdot r'w'$ or $rw \cdot a \cdot r'w' = rw \cdot b \cdot r'w'$.*

(b) *If $a \overset{*}{\Longrightarrow}_T b$, then also $rw \cdot a \cdot r'w' \overset{*}{\Longrightarrow}_T rw \cdot b \cdot r'w'$.*

Proof. Let $a = r_1x_1 \dotplus \cdots \dotplus r_mx_m$. Then there exist a rule $(u, v) \in T$ and strings $y, z \in X^*$ such that (u, v) reduces a at the monomial r_ix_i in order to get b. To simplify the notation we assume that $i = 1$, that is, $x_1 = yuz$ and $b = r_1yvz + (r_2x_2 \dotplus \cdots \dotplus r_mx_m)$.

Now $rw \cdot a \cdot r'w' = (rr_1r')wx_1w' + \cdots + (rr_mr')wx_mw'$. As the strings x_i are pairwise distinct, so are the strings wx_iw'. Thus, the above representation of $rw \cdot a \cdot r'w'$ is either a disjoint sum, and so

$$\begin{aligned} rw \cdot a \cdot r'w' &\Longrightarrow_T (rr_1r')wyvzw' + ((rr_2r')wx_2w' \dotplus \cdots \dotplus (rr_mr')wx_mw') \\ &= rw \cdot b \cdot r'w', \end{aligned}$$

or $rr_1r' = 0$, which implies that

$$\begin{aligned} rw \cdot b \cdot r'w' &= (rr_1r')wyvzw' + ((rr_2r')wx_2w' \dotplus \cdots \dotplus (rr_mr')wx_mw') \\ &= rw \cdot a \cdot r'w'. \end{aligned}$$

This proves (a). Part (b) simply follows by induction on the number of steps in the reduction $a \overset{*}{\Longrightarrow}_T b$. □

Even though the relation $\Longrightarrow_T$ itself is not compatible with addition, its reflexive, symmetric, and transitive closure $\overset{*}{\Longleftrightarrow}_T$ is a congruence on RX^*. In fact, we have the following result paralleling Theorem 3.3.

Theorem 4.4. *Let $T \subset X^* \times RX^*$. Then $\overset{*}{\Longleftrightarrow}_T \; = \Theta(T)$.*

Proof. First we show that $\overset{*}{\Longleftrightarrow}_T$ is a congruence on RX^*. Obviously, it is an equivalence relation. We claim that it also satisfies the substitution property. To verify this claim, it suffices to show that, for all $a, b, c \in RX^*$, if $a \Longrightarrow_T b$, then $a + c \overset{*}{\Longleftrightarrow}_T b + c$, $ac \overset{*}{\Longleftrightarrow}_T bc$, and $ca \overset{*}{\Longleftrightarrow}_T cb$ hold as well.

Assume that $a \Longrightarrow_T b$, and that (6) is satisfied. Let $c = s_1v_1 \dotplus \cdots \dotplus s_mv_m$. The following two cases are possible.

Case 1. $v_j \neq uwv$ for all $j = 1, \ldots, m$. Then

$$\begin{aligned} a + c &= ruwv \dotplus ((r_1u_1 \dotplus \cdots \dotplus r_ku_k) + (s_1v_1 \dotplus \cdots \dotplus s_mv_m)) \\ &\Longrightarrow_T ruw'v + (r_1u_1 \dotplus \cdots \dotplus r_ku_k) + (s_1v_1 \dotplus \cdots \dotplus s_mv_m) = b + c, \end{aligned}$$

and so $a + c \overset{*}{\Longleftrightarrow}_T b + c$.

Case 2. $v_j = uwv$ for some $j = 1, \ldots, m$. For simplicity we may assume that $v_1 = uwv$. There are two subcases.

Case 2.1. $r + s_1 \neq 0$. Then

$$\begin{aligned} a + c &= (r + s_1)uwv \dotplus ((r_1u_1 \dotplus \cdots \dotplus r_ku_k) + (s_2v_2 \dotplus \cdots \dotplus s_mv_m)) \\ &\Longrightarrow_T (r + s_1)uw'v + (r_1u_1 \dotplus \cdots \dotplus r_ku_k) + (s_2v_2 \dotplus \cdots \dotplus s_mv_m) \\ &\Longleftarrow_T s_1uwv \dotplus (ruw'v + r_1u_1 + \cdots + r_ku_k + s_2v_2 + \cdots + s_mv_m) \\ &= b + c, \end{aligned}$$

and so $a + c \overset{*}{\Longleftrightarrow}_T b + c$. Here we use the hypothesis that w does not appear in TERM(w'), and so s_1uwv is a direct summand of $b + c$.

Case 2.2. $r + s_1 = 0$. Then

$$\begin{aligned} a + c &= (r_1u_1 \dotplus \cdots \dotplus r_ku_k) + (s_2v_2 \dotplus \cdots \dotplus s_mv_m) \\ &= (r + s_1)uw'v + (r_1u_1 \dotplus \cdots \dotplus r_ku_k) + (s_2v_2 \dotplus \cdots \dotplus s_mv_m) \\ &\Longleftarrow_T s_1uwv \dotplus (ruw'v + r_1u_1 + \cdots + r_ku_k + s_2v_2 + \cdots + s_mv_m) \\ &= b + c, \end{aligned}$$

and so $a + c \overset{*}{\Longleftrightarrow}_T b + c$, too. As in Case 2.1 the hypothesis on (w, w') is used here.

Thus, in all these cases $a + c \overset{*}{\Longleftrightarrow}_T b + c$, and therefore $\overset{*}{\Longleftrightarrow}_T$ is compatible with addition.

In order to prove that $ac \overset{*}{\Longleftrightarrow}_T bc$, notice first that Lemma 4.3 implies that $a(sy) \overset{*}{\Longleftrightarrow}_T b(sy)$ holds for any $s \in R$ and $y \in X^*$. Since we have shown that $\overset{*}{\Longleftrightarrow}_T$ is compatible with addition, we obtain

$$\begin{aligned} ac &= as_1v_1 + as_2v_2 + \cdots + as_mv_m \\ &\overset{*}{\Longleftrightarrow}_T bs_1v_1 + as_2v_2 + \cdots + as_mv_m \\ &\overset{*}{\Longleftrightarrow}_T bs_1v_1 + bs_2v_2 + \cdots + as_mv_m \\ &\overset{*}{\Longleftrightarrow}_T \cdots \\ &\overset{*}{\Longleftrightarrow}_T bs_1v_1 + \cdots + bs_mv_m \\ &= bc. \end{aligned}$$

It can be shown similarly that $ca \overset{*}{\Longleftrightarrow}_T cb$ holds. Thus, $\overset{*}{\Longleftrightarrow}_T$ is indeed a congruence relation on RX^*. Moreover, since $T \subset \overset{*}{\Longleftrightarrow}_T$, it follows that $\Theta(T) \subseteq \overset{*}{\Longleftrightarrow}_T$.

To prove that $\overset{*}{\Longleftrightarrow}_T$ is contained in $\Theta(T)$, take any pair (a, b) with $a \Longrightarrow_T b$. Since $\Theta(T)$ is a congruence, (6) implies that $(a, b) \in \Theta(T)$. Since $\Theta(T)$ is an equivalence relation, it follows that $\overset{*}{\Longleftrightarrow}_T \subseteq \Theta(T)$. Hence, we see that $\overset{*}{\Longleftrightarrow}_T = \Theta(T)$, as required. □

Remark 4.5. The requirement that, for each rule, the left-hand side must not occur as a term in the corresponding right-hand side is essential for two reasons. First of all, if T contained a rule of the form $(u, ru \dotplus r_1u_1 \dotplus \cdots \dotplus r_ku_k)$, where $r, r_i \in R \smallsetminus \{0\}$ and $u, u_i \in X^*$, then $\Longrightarrow_T$ would in general not be terminating. Secondly, without this requirement the reduction relation $\Longrightarrow_T$ may not even generate the correct congruence relation. In fact, the following example shows that without this restriction the reflexive, symmetric, and transitive closure of $\Longrightarrow_T$ may not even be compatible with addition.

Example 4.6. Let $R := \mathbb{N}$, let $x, y \in X$, and let $T := \{(x, x + y)\}$. We claim that $x + x \overset{*}{\Longleftrightarrow}_T (x + y) + x$ does not hold, which shows that the relation $\overset{*}{\Longleftrightarrow}_T$ is not compatible with addition.

For all $a, b \in \mathbb{N}X^*$, if $a \Longrightarrow_T b$, then $\pi_b(y) = \pi_a(y) + \pi_a(x)$, and $\pi_b(z) = \pi_a(z)$ for all $z \in X \smallsetminus \{y\}$. Hence, for all integers $i \geq 0$, if $2x + iy \Longrightarrow_T b$, then $b = 2x + (i + 2)y$, and we obtain the following reduction sequences:

$$2x + y \Longrightarrow_T 2x + 3y \Longrightarrow_T 2x + 5y \Longrightarrow_T 2x + 7y \Longrightarrow_T \cdots, \qquad \text{and}$$
$$2x \Longrightarrow_T 2x + 2y \Longrightarrow_T 2x + 4y \Longrightarrow_T 2x + 6y \Longrightarrow_T \cdots.$$

Only the reductions indicated above are applicable to the elements of the above sequences. That is, if $a \Longrightarrow_T 2x+iy$, then $i \geq 2$, and $a = 2x+(i-2)y$. Thus, the elements $2x + y$ and $2x$ cannot be obtained as the result of a reduction, and the other elements of the sequences above can only be obtained by the indicated reduction steps. As the above sequences do not have any elements in common, it follows that $x + x \overset{*}{\Longleftrightarrow}_T (x + y) + x$ does not hold in $\mathbb{N}X^*$.

In the following we are concerned with the properties of the strong reduction relation that are central to the rewriting approach: termination and confluence. We will proceed as in Section 3, establishing first a sufficient condition for termination, consider the special case of T being a string rewriting system next, and finally discuss a test for (local) confluence in the general situation. As in Section 3.3 this test will be based on the notion of critical pair.

4.1. Termination

Suppose that a well-founded, admissible partial ordering $\succeq$ is given on X^*. By $\underline{\gg}$ we denote the well-founded partial ordering on the set of subsets of X^* that is induced by $\succeq$, which is in fact the restriction of the corresponding multiset ordering.

We now define a binary relation $\succeq^*$ on RX^* as follows:

$$p \succeq^* q \qquad \text{iff } \mathrm{TERM}(p) \;\underline{\gg}\; \mathrm{TERM}(q). \tag{7}$$

From this definition and the properties of the multiset ordering $\underline{\gg}$ we immediately obtain the following.

Proposition 4.7. *$\succeq^*$ is a well-founded quasi-ordering on RX^*.*

Based on this ordering we can easily derive the following result.

Theorem 4.8. *Let $\succeq$ be an admissible well-founded partial ordering on X^*, and let $T \subset X^* \times RX^*$ be a relation such that*

$$\forall (u, s_1v_1 \dotplus s_2v_2 \dotplus \cdots \dotplus s_mv_m) \in T\ \forall i = 1, \ldots, m\colon u \succ v_i. \tag{8}$$

Then $\Longrightarrow_T$ is terminating.

Proof. Assume that $a \Longrightarrow_T b$ holds. Then by (6)

$$a = rxuy \dotplus r_1u_1 \dotplus \cdots \dotplus r_nu_n,$$

and

$$b = (r \cdot s_1xv_1y \dotplus \cdots \dotplus r \cdot s_mxv_my) + (r_1u_1 \dotplus \cdots \dotplus r_nu_n),$$

where $(u, s_1v_1 \dotplus \cdots \dotplus s_mv_m)$ is the rule of T that is used in the reduction from a to b. Thus,

$$\mathrm{TERM}(a) = \{xuy, u_1, \ldots, u_n\}$$

and

$$\mathrm{TERM}(b) = \{xv_1y, \ldots, xv_my\} \cup \{u_1, \ldots, u_n\}.$$

By the hypothesis above $u \succ v_i$ for all $i = 1, \ldots, m$, and as the ordering $\succeq$ is admissible, we have $xuy \succ xv_iy$ for all $i = 1, \ldots, m$. Hence,

$$\mathrm{TERM}(a) \succ\!\!\succ \mathrm{TERM}(b),$$

that is, $a \succ^* b$, which shows that the quasi-ordering $\succeq^*$ is compatible with the reduction relation $\Longrightarrow_T$. As $\succeq^*$ is well-founded, this implies that $\Longrightarrow_T$ is terminating. □

4.2. Restricted reduction systems

Now we turn to the special case where $T \subset X^* \times X^*$. Then the relation T induces two reduction relations: the reduction relation $\longrightarrow_T$ on X^* defined by (3) and the strong reduction relation $\Longrightarrow_T$ on RX^* defined by (6). The following observation is straightforward.

Proposition 4.9. *Let (X, T) be a string rewriting system. Then the following conditions are equivalent for all strings $u, v \in X^*$:*

(a) $u \longrightarrow_T v$,

(b) $u \Longrightarrow_T v$.

Under what conditions does the reduction relation $\Longrightarrow_T$ inherit properties such as termination, local confluence or confluence from the relation $\longrightarrow_T$? For the termination property this is straightforward.

Corollary 4.10. *Let (X, T) be a finite string rewriting system. Then the relation $\Longrightarrow_T$ is terminating iff $\longrightarrow_T$ is terminating.*

Proof. If $\Longrightarrow_T$ is terminating, then so is $\longrightarrow_T$ by Proposition 4.9.

Conversely, if the reduction relation $\longrightarrow_T$ is terminating, then there exists an admissible well-founded partial ordering $\succeq$ on X^* that is compatible with $\longrightarrow_T$. Hence, Theorem 4.8 implies that $\Longrightarrow_T$ is also terminating. □

Next we establish a technical result that we will need for our further investigations.

Lemma 4.11. *Let (X, T) be a finite string rewriting system, and let*

$$a = r_1u_1 \dotplus \cdots \dotplus r_ku_k.$$

For $w \in X^*$, let $I_w(a) := \{i \in \{1, \ldots, k\} \mid u_i \xrightarrow{*}_T w\}$. Then

$$a \overset{*}{\Longrightarrow}_T \left(\sum_{i \in I_w(a)} r_i\right) w \dotplus \dot{\sum_{j \notin I_w(a)}} r_ju_j. \tag{9}$$

Proof. If $u_i \overset{*}{\longrightarrow}_T w$, then also $r_iu_i \overset{*}{\Longrightarrow}_T r_iw$. Hence,

$$\sum_{i \in I_w(a)} r_iu_i \overset{*}{\Longrightarrow}_T \left(\sum_{i \in I_w(a)} r_i\right) w.$$

All terms (or strings) x occurring in this reduction sequence reduce to w. Hence, none of them coincides with any of the u_j, $j \notin I_w(a)$. If

$$p = s_1x_1 \dotplus \cdots \dotplus s_mx_m$$

is a polynomial occurring in this reduction sequence, then

$$s_1x_1 \dotplus \cdots \dotplus s_mx_m + \dot{\sum_{j \notin I_w(a)}} r_ju_j$$

is actually a disjoint sum. Thus,

$$a = \dot{\sum_{i \in I_w(a)}} r_iu_i \dotplus \dot{\sum_{j \notin I_w(a)}} r_ju_j \overset{*}{\Longrightarrow}_T \left(\sum_{i \in I_w(a)} r_i\right) w \dotplus \dot{\sum_{j \notin I_w(a)}} r_ju_j. \quad \Box$$

Before continuing with the theory, we illustrate Lemma 4.11 by an example.

Example 4.12. Let $R := \mathbb{N}$, let $X := \{x, y\}$, and let $T := \{(xyx, xy)\}$. We consider the polynomial $a := 2xyxyx \dotplus 3xyxxy \dotplus xyyx$.

For $w := xyy$, we have

$$xyxyx \longrightarrow_T xyxy \longrightarrow_T xyy \qquad \text{and} \qquad xyxxy \longrightarrow_T xyxy \longrightarrow_T xyy,$$

while $xyyx$ does not reduce to xyy, and so,

$$a = 2xyxyx \dotplus 3xyxxy \dotplus xyyx \overset{*}{\Longrightarrow}_T 5xyy \dotplus xyyx.$$

On the other hand, for $w' := xyyx$, we have $xyxyx \longrightarrow_T xyyx$, while $xyxxy$ does not reduce to $xyyx$. Hence,

$$a = 2xyxyx \dotplus 3xyxxy \dotplus xyyx \overset{*}{\Longrightarrow}_T 3xyyx \dotplus 3xyxxy.$$

This example shows in particular that, for different strings w and w', the index sets $I_w(a)$ and $I_{w'}(a)$ are in general incomparable under inclusion.

Actually, for the case that $\longrightarrow_T$ is confluent, we have a stronger result.

Let $a = r_1u_1 \dotplus \cdots \dotplus r_nu_n$ be an element of RX^*. On the set of indices $I(a) := \{1, \ldots, n\}$, we define an equivalence relation $\sim$ as follows:

$$i \sim j \qquad \text{iff } u_i \overset{*}{\longleftrightarrow}_T u_j.$$

Further, by $P_T(a)$ we denote the partition of $I(a)$ that is induced by this equivalence relation.

Example 4.13. Let $R := \mathbb{N}$, let $X := \{x, y\}$, and let

$$T := \{(xyx, xy), (xyy, xy), (yyx, yyxx)\}.$$

Then $\longrightarrow_T$ is not terminating, but it can be shown to be confluent. Let

$$a := y^2x^3yx \dotplus 2y^2x^2y^2 \dotplus y^2x^2y \dotplus 3y^2x \dotplus 2xy^2 \dotplus 4xy.$$

Then $y^2x^3yx, y^2x^2y^2, y^2x^2y$ have the common descendant y^2x^3y, and xy^2, xy have the common descendant xy, while no other two terms of a are congruent mod $\longleftrightarrow_T$. Hence, $P_T(a) = \{\{1, 2, 3\}, \{4\}, \{5, 6\}\}$.

Lemma 4.14. *Let $a = r_1u_1 \dot{+} \cdots \dot{+} r_nu_n$ be an element of RX^*, and let $P_T(a) = \{U_1, \ldots, U_k\}$. If the relation $\longrightarrow_T$ is confluent (on X^*), then there exist strings $w_1, \ldots, w_k \in X^*$ such that*

$$a \overset{*}{\Longrightarrow}_T g_1w_1 \dot{+} g_2w_2 \dot{+} \cdots \dot{+} g_kw_k$$

holds, where $g_j := \sum_{i \in U_j} r_i$, $j = 1, \ldots, k$.

Proof. From the definition of $\sim$ we see that all the strings u_i, $i \in U_1$, are congruent mod $\overset{*}{\longleftrightarrow}_T$. As $\longrightarrow_T$ is confluent by our hypothesis, we see that there exists a string w_1 such that $u_i \overset{*}{\longrightarrow}_T w_1$ holds for each string u_i, $i \in U_1$. Further, if x is a string u_s or any of its descendants, where $s \notin U_1$, then x cannot be reduced to w_1. Hence, we see from Lemma 4.11 that

$$a \overset{*}{\Longrightarrow}_T g_1w_1 \dot{+} \dot{\sum_{j \notin U_1}} r_ju_j.$$

By repeating this argument for each index $j = 2, \ldots, k$, we obtain the result above. □

Example 4.13 (Continued). As $y^2x^3yx, y^2x^2y^2, y^2x^2y$ have the common descendant y^2x^3y, and xy^2, xy have the common descendant xy, we obtain that

$$\begin{aligned} a &= y^2x^3yx \dot{+} 2y^2x^2y^2 \dot{+} y^2x^2y \dot{+} 3y^2x \dot{+} 2xy^2 \dot{+} 4xy \\ &\overset{*}{\Longrightarrow}_T 4y^2x^3y \dot{+} 3y^2x \dot{+} 6xy. \end{aligned}$$

Next we turn to the property of local confluence.

Theorem 4.15. *Let (X, T) be a finite string rewriting system. Then the reduction relation $\Longrightarrow_T$ on RX^* is locally confluent iff $\longrightarrow_T$ is locally confluent.*

Proof. If $\Longrightarrow_T$ is locally confluent, then so is $\longrightarrow_T$ by Proposition 4.9. Thus, it remains to consider the converse implication.

Let a, b, c be three elements of RX^* such that $a \Longrightarrow_T b$ and $a \Longrightarrow_T c$, and let a have the following representation as a disjoint sum:

$$a = r_1u_1 \dot{+} \cdots \dot{+} r_ku_k.$$

First, suppose that b and c are obtained from a by rewriting the same monomial, say u_1. That is, there are x_1 and y_1 such that $u_1 \longrightarrow_T x_1$ and $u_1 \longrightarrow_T y_1$, where

$$\begin{aligned} b &= r_1x_1 + r_2u_2 + \cdots + r_ku_k, \\ c &= r_1y_1 + r_2u_2 + \cdots + r_ku_k. \end{aligned}$$

Since $\longrightarrow_T$ is locally confluent, there exists some $w \in X^*$ such that $x_1 \overset{*}{\longrightarrow}_T w$ and $y_1 \overset{*}{\longrightarrow}_T w$. By Lemma 4.11 this yields

$$b \overset{*}{\Longrightarrow}_T b' := \left(r_1 + \sum_{i \in I_w(a) \setminus \{1\}} r_i \right) w \dot{+} \dot{\sum_{j \notin I_w(a)}} r_j u_j, \qquad \text{and}$$

$$c \overset{*}{\Longrightarrow}_T c' := \left(r_1 + \sum_{i \in I_w(a) \setminus \{1\}} r_i \right) w \dot{+} \dot{\sum_{j \notin I_w(a)}} r_j u_j.$$

As $b' = c'$, we see that b and c have a common descendant, and local confluence holds in this case.

Secondly, suppose that b and c are obtained from a by rewriting distinct monomials, say u_1 and u_2. That is, there exist x_1, x_2 such that $u_1 \longrightarrow_T x_1$ and $u_2 \longrightarrow_T x_2$, and

$$b = r_1 x_1 + r_2 u_2 + r_3 u_3 + \cdots + r_k u_k,$$
$$c = r_1 u_1 + r_2 x_2 + r_3 u_3 + \cdots + r_k u_k.$$

In this situation two cases are possible.

Case 1. x_1 and x_2 have a common descendant w. Then

$$b \overset{*}{\Longrightarrow}_T b' := \left(r_1 + r_2 + \sum_{i \in I_w(a) \setminus \{1,2\}} r_i \right) w \dot{+} \dot{\sum_{j \notin I_w(a)}} r_j u_j, \qquad \text{and}$$

$$c \overset{*}{\Longrightarrow}_T c' := \left(r_1 + r_2 + \sum_{i \in I_w(a) \setminus \{1,2\}} r_i \right) w \dot{+} \dot{\sum_{j \notin I_w(a)}} r_j u_j.$$

As $b' = c'$, local confluence also follows in this case.

Case 2. x_1 and x_2 do not have a common descendant. In particular, this means that $x_1 \neq u_2$ and $x_2 \neq u_1$ hold. Hence,

$$b = r_2 u_2 \dot{+} (r_1 x_1 + r_3 u_3 + \cdots + r_k u_k) \Longrightarrow_T r_1 x_1 + r_2 x_2 + r_3 u_3 + \cdots + r_k u_k$$

and

$$c = r_1 u_1 \dot{+} (r_2 x_2 + r_3 u_3 + \cdots + r_k u_k) \Longrightarrow_T r_1 x_1 + r_2 x_2 + r_3 u_3 + \cdots + r_k u_k.$$

Thus, also in this case b and c have a common descendant. As this covers all possible cases, it follows that $\Longrightarrow_T$ is indeed locally confluent, if $\longrightarrow_T$ is. □

By combining Corollary 4.10 and Theorem 4.15 we obtain the following result.

Corollary 4.16. *Let (X, T) be a finite string rewriting system. Then $\longrightarrow_T$ is convergent iff $\Longrightarrow_T$ is convergent. If these relations are convergent, then the unique normal form for $a = r_1 u_1 \dot{+} \cdots \dot{+} r_k u_k$ is of the form $r_1 \hat{u}_1 + \cdots + r_k \hat{u}_k$, where $\hat{u}_i$ is the unique normal form of the string u_i* mod $\longrightarrow_T$.

Here the result on the form of the normal forms follows from the fact that a string $u \in X^*$ is irreducible mod $\longrightarrow_T$ iff it is irreducible mod $\Longrightarrow_T$ and from Lemma 4.14.

Corollary 4.17. *Let (X, T) be a finite string rewriting system, and let R be a semiring such that computations in R can be performed effectively. If $\longrightarrow_T$ is convergent, then the congruence $\Theta(T)$ is decidable in RX^*.*

Proof. By Corollary 4.16 the reduction relation $\Longrightarrow_T$ is convergent on RX^*. As it is effectively computable, it follows that the equivalence relation $\overset{*}{\Longleftrightarrow}_T$ is decidable. By Theorem 4.4, $\overset{*}{\Longleftrightarrow}_T$ coincides with $\Theta(T)$. □

Next we generalize Theorem 4.15 to the notion of confluence.

Theorem 4.18. *Let (X, T) be a finite string rewriting system. Then the reduction relation $\Longrightarrow_T$ on RX^* is confluent iff $\longrightarrow_T$ is confluent.*

Proof. If $\Longrightarrow_T$ is confluent, then so is $\longrightarrow_T$ by Proposition 4.9. Thus, it remains to consider the converse implication.

So let $a, b, c \in RX^*$ such that $a \overset{*}{\Longrightarrow}_T b$ and $a \overset{*}{\Longrightarrow}_T c$ hold. By Lemma 4.14 there exist strings $x_1, \ldots, x_k$ and integers $g_1, \ldots, g_k$ such that

$$b \overset{*}{\Longrightarrow}_T g_1 x_1 \dot{+} \cdots \dot{+} g_k x_k,$$

and x_i is not congruent to x_j for $i \neq j$. Further, g_i is the sum of the coefficients of all those monomials in b for which the terms are congruent to x_i mod $\overset{*}{\longleftrightarrow}_T$. Analogously, there exist strings $y_1, \ldots, y_p$ and integers $h_1, \ldots, h_p$ such that

$$c \overset{*}{\Longrightarrow}_T h_1 y_1 \dot{+} \cdots \dot{+} h_p y_p,$$

and y_i is not congruent to y_j for $i \neq j$. Further, h_i is the sum of the coefficients of all those monomials in c for which the terms are congruent to y_i mod $\overset{*}{\longleftrightarrow}_T$.

As $a \overset{*}{\Longrightarrow}_T b$ and $a \overset{*}{\Longrightarrow}_T c$ both hold, we see that $p = k$, and that there is a bijection $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k\}$ such that $x_i \overset{*}{\longleftrightarrow}_T y_{\sigma(i)}$ and $g_i = h_{\sigma(i)}$ hold. As $\longrightarrow_T$ is confluent, there exists a string w_i such that $x_i \overset{*}{\longrightarrow}_T w_i$ and $y_{\sigma(i)} \overset{*}{\longrightarrow}_T w_i$ both hold, $i = 1, \ldots, k$. Thus, b and c both reduce to $d := g_1 w_1 \dot{+} \cdots \dot{+} g_k w_k$. Hence, with $\longrightarrow_T$ also $\Longrightarrow_T$ is confluent. □

4.3. Test for (local) confluence

For the special case of systems of the form $T \subset X^* \times X^*$ the results of the previous subsection show that local confluence of the reduction relation $\Longrightarrow_T$ on RX^* is equivalent to the local confluence of the relation $\longrightarrow_T$ on X^*, and therewith it is characterized by the critical pairs of the string rewriting system T. In particular, for finite terminating systems T, this means that (local) confluence is decidable (see, e.g., Book and Otto, 1993, Theorem 2.3.1).

Here we want to investigate the problem of testing (local) confluence for reduction relations $\Longrightarrow_T$ on RX^* that are generated by more general systems than string rewriting systems. In fact, we return to systems of the form $T \subset X^* \times RX^*$, that is, each element of T

is of the form $(u, r_1v_1 \dotplus r_2v_2 \dotplus \cdots \dotplus r_mv_m)$, where $u, v_1, \ldots, v_m \in X^*, r_1, \ldots, r_m \in R$, and $m \geq 0$.

We assume that $\succeq$ is an admissible well-founded partial ordering on X^*, and that T satisfies condition (8). Then, by Theorem 4.8, the reduction relation $\Longrightarrow_T$ is terminating. Hence, in this setting local confluence coincides with confluence. We will establish a characterization of confluence for $\Longrightarrow_T$ that is based on the notion of critical pairs.

Let

$$(u_1, r_1v_1 \dotplus r_2v_2 \dotplus \cdots \dotplus r_kv_k) \quad \text{and} \quad (u_2, s_1w_1 \dotplus s_2w_2 \dotplus \cdots \dotplus s_pw_p) \qquad (10)$$

be two (not necessarily distinct) elements of T.

The rules overlap in the same situation as in Definition 3.15, and the resulting critical pairs are obtained analogously to Definition 3.17. That is, if there exist strings $x, y \in X^*$, $0 < |x| < |u_2|$, such that $u_1x = yu_2$, then the monomial u_1x can be rewritten by both rules:

$$u_1x \Longrightarrow_T r_1v_1x \dotplus r_2v_2x \dotplus \cdots \dotplus r_kv_kx$$

and

$$u_1x = yu_2 \Longrightarrow_T s_1yw_1 \dotplus s_2yw_2 \dotplus \cdots \dotplus s_pyw_p.$$

Also if there exist strings $x, y \in X^*$ such that $u_1 = xu_2y$, then the monomial u_1 can be rewritten by both rules:

$$u_1 \Longrightarrow_T r_1v_1 \dotplus r_2v_2 \dotplus \cdots \dotplus r_kv_k$$

and

$$u_1 = xu_2y \Longrightarrow_T s_1xw_1y \dotplus s_2xw_2y \dotplus \cdots \dotplus s_pxw_py.$$

Accordingly, we obtain the critical pair

$$(r_1v_1x + r_2v_2x + \cdots + r_kv_kx, s_1yw_1 + s_2yw_2 + \cdots + s_pyw_p),$$

if $u_1x = yu_2$ for some $x, y \in X^*$, $0 < |x| < |u_2|$, and

$$(r_1v_1 + r_2v_2 + \cdots + r_kv_k, s_1xw_1y + s_2xw_2y + \cdots + s_pxw_py),$$

if $u_1 = xu_2y$ for some $x, y \in X^*$. As before $\mathrm{CP}(T)$ denotes the set of all critical pairs of T. Further, we denote by $\mathrm{IRR}(\Longrightarrow_T)$ the set of all irreducible elements of RX^* mod $\Longrightarrow_T$.

Based on these notions we derive the following characterization of confluence. In contrast to Theorem 3.18 this characterization is obtained only for the special case that the reduction relation $\Longrightarrow_T$ is terminating. Also it is required that the underlying semiring is commutative with respect to multiplication.

Theorem 4.19. *Let R be a commutative semiring, and let $T \subset X^* \times RX^*$ be a system of rules that satisfies condition* (8) *above. Then the following statements are equivalent:*

(a) *The relation $\Longrightarrow_T$ is confluent on RX^*.*

(b) *The polynomials p and q have a common descendant* mod $\Longrightarrow_T$ *for each pair $(p, q) \in \mathrm{CP}(T)$.*

Proof. By Theorem 4.8 the reduction relation $\Longrightarrow_T$ is terminating, and so confluence is equivalent to local confluence. Certainly, if $\Longrightarrow_T$ is (locally) confluent, then p and q must have a common descendant mod $\Longrightarrow_T$ for each critical pair (p, q) of T. Thus, it remains to prove the converse implication.

Now assume conversely that each critical pair of T resolves. We claim that each polynomial $a \in RX^*$ has a unique irreducible descendant mod $\Longrightarrow_T$. For proving this we proceed by Noetherian induction based on the quasi-ordering $\succeq^*$ on RX^* defined in (7).

Certainly each irreducible polynomial has a unique normal form. So let $a = r_1x_1 \dot{+} \cdots \dot{+} r_mx_m$ be a reducible polynomial such that each polynomial d satisfying $d \,{}^*\!\!\prec a$ has a unique normal form. We will also show that a has a unique normal form. For that we have to consider various cases.

Case 1. There is only a single possible reduction that applies to a. Then there is a unique polynomial b such that $a \Longrightarrow_T b$. By (8), $b \,{}^*\!\!\prec a$, and so b has a unique normal form by our induction hypothesis, which then is also the unique normal form of a.

Case 2. There are two or more reductions that apply to a.

Case 2.1. Assume that a is a monomial, that is, $a = r_1u_1$. Further, let $a \Longrightarrow_T b \overset{*}{\Longrightarrow}_T \hat{b} \in \mathrm{IRR}(\Longrightarrow_T)$. We need to show that $\hat{b}$ is the only irreducible descendant of a. So let $a \Longrightarrow_T c$ be another reduction step.

Case 2.1.1. The steps $a \Longrightarrow_T b$ and $a \Longrightarrow_T c$ rewrite non-overlapping factors of the term u_1. More precisely, there exist rules (ℓ_1, v_1) and (ℓ_2, v_2) in T and strings $x, y, z \in X^*$ such that $u_1 = x\ell_1y\ell_2z$. Then the monomial r_1u_1 has the two immediate descendants $r_1xv_1y\ell_2z$ and $r_1x\ell_1yv_2z$.

Assume that

$$v_1 = s_1v_{1,1} \dot{+} \cdots \dot{+} s_kv_{1,k}$$

and

$$v_2 = t_1v_{2,1} \dot{+} \cdots \dot{+} t_nv_{2,n}$$

for some integers $k, n \geq 0$. Hence,

$$r_1xv_1y\ell_2z = (r_1s_1)xv_{1,1}y\ell_2z \dot{+} \cdots \dot{+} (r_1s_k)xv_{1,k}y\ell_2z$$

and

$$r_1x\ell_1yv_2z = (r_1t_1)x\ell_1yv_{2,1}z \dot{+} \cdots \dot{+} (r_1t_n)x\ell_1yv_{2,n}z.$$

As these representations are disjoint sums, it is easily seen that

$$\begin{aligned} r_1xv_1y\ell_2z &\overset{*}{\Longrightarrow}_T (r_1s_1)xv_{1,1}yv_2z + \cdots + (r_1s_k)xv_{1,k}yv_2z \\ &= \sum_{i=1}^{k}\sum_{j=1}^{n}(r_1s_it_j)xv_{1,i}yv_{2,j}z \end{aligned}$$

and

$$\begin{aligned} r_1 x \ell_1 y v_2 z &\overset{*}{\Longrightarrow}_T (r_1 t_1) x v_1 y v_{2,1} z + \cdots + (r_1 t_n) x v_1 y v_{2,n} z \\ &= \sum_{i=1}^{k} \sum_{j=1}^{n} (r_1 t_j s_i) x v_{1,i} y v_{2,j} z. \end{aligned}$$

As the semiring R is commutative, we have $s_i t_j = t_j s_i$, and therefore, the two immediate descendants of $r_1 u_1$ have a common descendant. However, $b \stackrel{*}{\prec} a$ and $c \stackrel{*}{\prec} a$, and so b and c each only have a single normal form. Thus, they both have the same normal form, which is the polynomial $\hat{b}$.

Case 2.1.2. The steps $a \Longrightarrow_T b$ and $a \Longrightarrow_T c$ form an instance of a critical pair, that is, $b = r_1 x \cdot p \cdot y$ and $c = r_1 x \cdot q \cdot y$ for some $x, y \in X^*$ and $p, q \in RX^*$ such that $(p, q) \in \mathrm{CP}(T)$. By condition (b), the critical pair (p, q) resolves to a common descendant $d \in RX^*$. Then based on Lemma 4.3 it follows that b and c have a common descendant, $r_1 x \cdot d \cdot y$, which as in the subcase above implies that $\hat{b}$ is the unique normal form of both b and c.

Thus, we see that in this case a has the unique normal form $\hat{b}$.

Case 2.2. Assume that $a = r_1 u_1 \dotplus \cdots \dotplus r_k u_k$ for some $k > 1$. Again let

$$a \Longrightarrow_T b \Longrightarrow_T^* \hat{b} \in \mathrm{IRR}(\Longrightarrow_T)$$

and let $a \Longrightarrow_T c$ be another reduction step.

Case 2.2.1. Let us suppose first that b and c are obtained from a by rewriting at different monomials, say u_1 and u_2. That is, there exist polynomials $v = \sum s_i v_i$ and $w = \sum t_i w_i$ such that $u_1 \Longrightarrow_T v$ and $u_2 \Longrightarrow_T w$ and

$$\begin{aligned} b &= r_1 v + r_2 u_2 + \cdots + r_k u_k, \\ c &= r_1 u_1 + r_2 w + \cdots + r_k u_k. \end{aligned}$$

If $u_2 \notin \mathrm{TERM}(v)$ and $u_1 \notin \mathrm{TERM}(w)$, then $r_2 u_2$ is a direct summand of b, and $r_1 u_1$ is a direct summand of c, and hence

$$b \Longrightarrow_T r_1 v + r_2 w + \cdots + r_k u_k \Longleftarrow_T c.$$

Assume now that $u_2 \in \mathrm{TERM}(v)$, say $u_2 = v_i$ for some i. It follows that $(r_2 + r_1 s_i) u_2$ is a direct summand of b, and we get the following:

$$\begin{aligned} b \ &= (r_2 + r_1 s_i) u_2 \dotplus \left(r_1 \sum_{j \neq i} s_j v_j + r_3 u_3 + \cdots + r_k u_k \right) \\ &\Longrightarrow_T (r_2 + r_1 s_i) w + \left(r_1 \sum_{j \neq i} s_j v_j + r_3 u_3 + \cdots + r_k u_k \right) =: b'. \end{aligned}$$

On the other hand, since $u_2 = v_i$, condition (8) implies $u_1 \succ u_2$, because the ordering $\succeq$ is admissible. It follows that $u_1 \notin \mathrm{TERM}(w)$, and so $r_1 u_1$ is a direct summand of c.

Therefore we obtain the following:

$$\begin{aligned} c &= r_1u_1 \dotplus (r_2w + \cdots + r_ku_k) \\ &\Longrightarrow_T r_1v + (r_2w + \cdots + r_ku_k) \\ &= (r_1s_iv_i) \dotplus \left(r_1 \sum_{j\neq i} s_jv_j + r_2w + r_3u_3 + \cdots + r_ku_k\right) \\ &\Longrightarrow_T (r_1s_iw) + \left(r_1 \sum_{j\neq i} s_jv_j + r_2w + r_3u_3 + \cdots + r_ku_k\right) \\ &= (r_2 + r_1s_i)w + \left(r_1 \sum_{j\neq i} s_jv_j + r_3u_3 + \cdots + r_ku_k\right) \\ &= b'. \end{aligned}$$

Hence, b and c have a common descendant, whenever they are obtained from a by rewriting at different monomials. However, as $b \;{}^*\!\!\prec a$ and $c \;{}^*\!\!\prec a$, we obtain from the induction hypothesis that b and c each have a unique normal form, which is $\hat{b}$.

Case 2.2.2. The two reductions $a \Longrightarrow_T b$ and $a \Longrightarrow_T c$ rewrite the same monomial of a, say r_1u_1. If there is another monomial of a that is reducible, then by considering the polynomial d obtained in a single step by reducing a at one such monomial we obtain from the Case 2.2.1 that b and d have the same unique normal form, and that c and d have the same unique normal form. Thus, all these polynomials have the unique normal form $\hat{b}$.

If no other monomial of a is reducible, then $d := r_2u_2 \dotplus \cdots \dotplus r_ku_k$ is irreducible. Further, $b = r_1v + d$ and $c = r_1w + d$, where r_1v and r_1w are the polynomials obtained by reducing the monomial r_1u_1. Now $r_1u_1 \;{}^*\!\!\prec a$, and so r_1u_1 has a unique normal form u by our induction hypothesis, which is also the unique normal form of r_1v and of r_1w. Thus, $r_1v \overset{*}{\Longrightarrow}_T u$ and $r_1w \overset{*}{\Longrightarrow}_T u$. As d is a sum of irreducible monomials, we see that the monomials of d do not interfere with these reductions, that is, $b = r_1v + d \overset{*}{\Longrightarrow}_T u + d$ and $c = r_1w + d \overset{*}{\Longrightarrow}_T u + d$. Thus, also in this case b and c have a common descendant, and therewith we can again apply the induction hypothesis which yields that b and c have the same unique normal form $\hat{b}$.

As this covers all cases we see that a has a unique normal form, and so by Noetherian induction it follows that each polynomial from RX^* has a unique normal form. Thus, the reduction relation $\Longrightarrow_T$ is indeed confluent. □

We close this subsection with two short examples.

Example 4.20. Let $R := \mathbb{Z}$, $X := \{x, y, z\}$, and T consist of the following four ‘rules’:

(1) $x^2 \to y + z$,

(2) $yx \to xy + 3x$,

(3) $zx \to xz - 3x$,

(4) $zy \to yz - 6y - 6z$.

If $\succeq$ is the length-lexicographical ordering in X^* that is induced by the linear ordering $z > y > x$ on X, then we see that T satisfies condition (8). There are four overlaps between the rules of T, resulting in four critical pairs:

$$\begin{aligned}
&xy + xz \Longleftarrow_{(1)} x \cdot x^2 = x^2 \cdot x \Longrightarrow_{(1)} yx + zx,\\
&y^2 + yz \Longleftarrow_{(1)} y \cdot x^2 = yx \cdot x \Longrightarrow_{(2)} xyx + 3x^2,\\
&zy + z^2 \Longleftarrow_{(1)} z \cdot x^2 = zx \cdot x \Longrightarrow_{(3)} xzx - 3x^2,\\
&zxy + 3zx \Longleftarrow_{(2)} z \cdot yx = zy \cdot x \Longrightarrow_{(4)} yzx - 6yx - 6zx.
\end{aligned}$$

These critical pairs resolve as follows. The first pair $(xy + xz, yx + zx)$ resolves, as $yx + zx \Longrightarrow_{(2)} xy + 3x + zx \Longrightarrow_{(3)} xy + 3x + xz - 3x = xy + xz$.

The second pair $(y^2 + yz, xyx + 3x^2)$ resolves, as

$$\begin{aligned}
xyx + 3x^2 &\Longrightarrow_{(2)} x^2y + 6x^2 \Longrightarrow_{(1)} y^2 + zy + 6x^2\\
&\Longrightarrow_{(4)} y^2 + yz - 6y - 6z + 6x^2 \Longrightarrow_{(1)} y^2 + yz.
\end{aligned}$$

The third pair $(zy + z^2, xzx - 3x^2)$ resolves, as

$$\begin{aligned}
xzx - 3x^2 &\Longrightarrow_{(3)} x^2z - 6x^2 \Longrightarrow_{(1)} yz + z^2 - 6x^2\\
&\Longrightarrow_{(1)} yz + z^2 - 6y - 6z \Longleftarrow_{(4)} zy + z^2,
\end{aligned}$$

and the fourth pair $(zxy + 3zx, yzx - 6yx - 6zx)$ resolves, as

$$\begin{aligned}
zxy + 3zx &\Longrightarrow_{(3)} xzy - 3xy + 3zx \Longrightarrow_{(4)} xyz - 9xy - 6xz + 3zx\\
&\Longrightarrow_{(3)} xyz - 9xy - 3xz - 9x
\end{aligned}$$

and

$$\begin{aligned}
yzx - 6yx - 6zx &\Longrightarrow_{(3)} yxz - 9yx - 6zx\\
&\Longrightarrow_{(2)} xyz + 3xz - 9yx - 6zx\\
&\Longrightarrow_{(3)} xyz - 9yx - 3xz + 18x\\
&\Longrightarrow_{(2)} xyz - 9xy - 3xz - 9x.
\end{aligned}$$

Thus, the reduction relation $\Longrightarrow_T$ is convergent.

The commutativity of the semiring is essential for ensuring that it suffices to resolve all the critical pairs in order to guarantee confluence of the reduction relation. This is illustrated by the following example.

Example 4.21. Let R be a semiring, let $r, s \in R$ such that $rs \neq sr$, let $x, x'y, y' \in X$ be distinct elements of X, and let $T := \{(x, rx'), (y, sy')\}$. Then $\mathrm{CP}(T) = \emptyset$, but the reduction relation $\Longrightarrow_T$ is not confluent, as the element xy has two different irreducible descendants:

$$xy \Longrightarrow_T rx'y \Longrightarrow_T rsx'y' \qquad \text{and} \qquad xy \Longrightarrow_T sxy' \Longrightarrow_T srx'y'.$$

5. Computing normal forms

If $T \subset X^* \times RX^*$ is a finite set of rules such that the weak reduction relation $=\!\!\Longrightarrow_T$ or the strong reduction relation $\Longrightarrow_T$ is convergent, then the congruence $\Theta(T)$ can be characterized as follows: two polynomials $p, q \in RX^*$ are congruent mod $\Theta(T)$ iff the unique normal forms $\hat{p}$ of p and $\hat{q}$ of q with respect to $\mathrel{=\!\!=\!\!\!>}_T$ or $\Longrightarrow_T$, respectively, coincide. Hence, if computations in the semiring R can be performed effectively, the membership problem for the congruence $\Theta(T)$ reduces to the problem of computing normal forms.

Analogously, if T is terminating, then (local) confluence of $\mathrel{=\!\!=\!\!\!>}_T$ (Theorem 3.18) and of $\Longrightarrow_T$ (Theorem 4.19) has been characterized by the technical condition that, for each critical pair (p, q) of T, p and q have a common descendant, provided some additional restrictions apply. However, instead of determining all the descendants of p and of q and then to check whether these sets have a non-empty intersection, it suffices to determine arbitrary normal forms $\hat{p}$ of p and $\hat{q}$ of q. If these normal forms coincide, then obviously p and q have a common descendant; otherwise, T is certainly not (locally) confluent. Thus, also the task of checking (local) confluence reduces to the problem of computing normal forms.

If T is terminating, then an arbitrary reduction strategy can be used to reduce a given polynomial to normal form. However, as this process can be very time consuming, one is interested in strategies that are as efficient as possible. Certainly the *derivational complexity* of T gives a lower bound for the complexity of the process of computing normal forms. Here, with a terminating system T, we associate its *complexity function* $D_T : \mathbb{N} \to \mathbb{N}$, which is defined by

$$D_T(n) := \max\{d_T(p) \mid p \in RX^*, |p| \leq n\},$$

where $d_T : RX^* \to \mathbb{N}$ is defined as

$$d_T(p) := \min\{k \mid \exists p_0, \ldots, p_k\colon p = p_0 \Longrightarrow_T p_1 \Longrightarrow_T \cdots \Longrightarrow_T p_k \in \mathrm{IRR}(T)\},$$

and $|p|$ denotes the *size* of p in some natural encoding. For example, if $p = r_1u_1 \dotplus \cdots \dotplus r_nu_n$, where $r_i \in \mathbb{N}$ and $u_i \in X^*$, then

$$|p| := \sum_{i=1}^{n} (|\mathrm{bin}(r_i)| + |u_i|)$$

is an obvious choice, where $\mathrm{bin}(r_i)$ is the binary encoding of the coefficient r_i and $|u_i|$ denotes the length of the string u_i.

If T is a string rewriting system, that is, $T \subset X^* \times X^*$, then the complexity of actually computing a normal form of a string u depends linearly on the length of the reduction sequence from u to the normal form $\hat{u}$ computed (see, e.g., Book and Otto, 1993, Section 2.2). The length of this sequence, on the other hand, depends on the reduction strategy used. However, an upper bound can be obtained from the partial ordering that is used to verify the termination of T. If T is weight-reducing, then $d_T(u) \leq g(u)$, where g is the corresponding *weight-function*, if T is compatible with a length-lexicographical ordering, then $d_T(u) \leq c^{|u|}$ for some constant $c > 1$, but much higher bounds are possible, and in many cases these bounds are actually sharp (Hofbauer, 1992).

For systems of the form $T \subset X^* \times RX^*$, the situation is even more involved, as a reduction step $p \Longrightarrow_T q$ replaces a monomial ru of p by a sum of monomials $rs_1u_1 \dotplus \cdots \dotplus rs_nu_n$, and subsequently all these monomials have to be reduced to normal form. This makes it clear that in general the process of reducing a polynomial to normal form is very time consuming. This has also been observed in many experiments with Buchberger's algorithm for computing Groebner bases, where it turned out that the most time was spent in normal form computations (see, e.g., Gebauer and Möller, 1988).

To conclude this discussion we present a particular reduction strategy for free monoid semirings. For such a strategy we must make several choices:

(1) If $p = r_1u_1 \dotplus \cdots \dotplus r_nu_n$ is the polynomial that is to be reduced to normal form, then we have to choose a monomial r_iu_i from among all the reducible monomials of p.
(2) Once we have chosen a monomial r_iu_i, we have to choose a rule $(u, q) \in T$ from among all the rules that are applicable to this monomial.
(3) Once we have chosen a monomial r_iu_i and a rule $(u, q) \in T$, we have to choose a factorization of u_i of the form $u_i = xuy$ $(x, y \in X^*)$ from among all such factorizations.

Of course, the first two choices can be made in reverse order, choosing first a rule of T that applies to one or more monomials of p, and then pick one of these monomials. Also other orders are possible.

Our strategy is obtained by choosing specific instantiations of the choices above:

(1) From among the reducible monomials of p, we choose a maximal one with respect to the partial ordering $\succeq$ that is used for proving termination of T. That is, if the monomial r_iu_i is chosen, then for all $j \neq i$, r_ju_j is either irreducible, or $u_j \succ u_i$ does not hold.
(2) From among the rules of T that apply to the chosen monomial r_iu_i, we choose a rule (u, q) such that TERM(q) is minimal with respect to the induced multiset ordering $\underline{\gg}$.
(3) From among the various factorizations of the form $u_i = xuy$, we choose the leftmost one. That is, if $u_i = xuy = vuw$, where $x, y, v, w \in X^*$ and $(u, q) \in T$, then we choose xuy if $|x| < |v|$.

The rationale behind these choices is as follows.

(1) By reducing a large term, we obtain a collection of smaller terms. Some of these terms may coincide with other terms that already occur in the polynomial p, possibly cancelling them. Further, if we were to reduce a small term u first, then a later reduction step that replaces a larger term may reintroduce a monomial with term u, thus necessitating additional reduction steps.
(2) The motivation for this choice of the rule (u, q) to be applied is the desire to reduce the monomial r_iu_i by this one step as much as possible. The effect is measured in terms of the partial ordering $\underline{\gg}$.
(3) It appears reasonable to perform reductions within a term u_i either strictly from left to right or from right to left. We have chosen the first alternative in accordance with the way in which traditionally finite-state acceptors process strings.

We illustrate this strategy with an example.

Example 5.1. Let $R := \mathbb{Z}$, $X := \{x, y, z\}$, and let T be the system from Example 4.20 that consists of the following four 'rules':

(1) $x^2 \to y + z$,
(2) $yx \to xy + 3x$,
(3) $zx \to xz - 3x$,
(4) $zy \to yz - 6y - 6z$.

Further, let $p := zyx + 9yx$. Both terms of p are reducible, but with respect to the length-lexicographical ordering induced by $z > y > x$, zyx is the maximal reducible term. Rules (2) and (4) are both applicable to this term, but

$$\mathrm{TERM}(yz - 6y - 6z) = \{yz, y, z\} \succ\succ \{xy, x\} = \mathrm{TERM}(xy + 3x),$$

and so we choose rule (2). Hence, the first step according to our strategy is

$$p := zyx + 9yx \Longrightarrow_{(2)} zxy + 3zx + 9yx =: p_1.$$

All three terms of p_1 are reducible, but zxy is the maximal one. Only one rule is applicable to it, that is, the next reduction step is

$$p_1 = zxy + 3zx + 9yx \Longrightarrow_{(3)} xzy - 3xy + 3zx + 9yx =: p_2.$$

The maximal reducible term of p_2 is xzy. As only rule (4) applies to it, the next reduction step yields

$$\begin{aligned} p_2 &= xzy - 3xy + 3zx + 9yx \\ &\Longrightarrow_{(4)} xyz - 6xy - 6xz - 3xy + 3zx + 9yx \\ &= xyz - 9xy - 6xz + 3zx + 9yx =: p_3. \end{aligned}$$

The polynomial p_3 contains two terms that are still reducible: zx and yx. As $z > y$, zx is the maximal reducible term, and so the next reduction step is

$$\begin{aligned} p_3 &= xyz - 9xy - 6xz + 3zx + 9yx \\ &\Longrightarrow_{(3)} xyz - 9xy - 6xz + 3xz - 9x + 9yx \\ &= xyz - 9xy - 3xz - 9x + 9yx =: p_4. \end{aligned}$$

Finally, yx is the only remaining term that is reducible, and so the final reduction step is

$$\begin{aligned} p_4 &= xyz - 9xy - 3xz - 9x + 9yx \\ &\Longrightarrow_{(2)} xyz - 9xy - 3xz - 9x + 9xy + 27x \\ &= xyz - 3xz + 18x =: p_5, \end{aligned}$$

which yields the normal form $p_5 = xyz - 3xz + 18x$ of p.

It is conceivable that instead of choosing the rule (u, q) of T to be applied to the chosen monomial $r_i u_i$ based on the set $\mathrm{TERM}(q)$, one could also take into account the effect of applying that rule. For example, one could choose a rule (u, q) and a factorization xuy of u_i in such a way that the set $\mathrm{TERM}(xqy)$ is minimal with respect to the induced multiset ordering $\underline{\gg}$. This, however, amounts essentially to the process of applying all possible reduction steps to the term u_i and then choosing the one that yields the best (that is, minimal) result, which appears to be quite an expensive strategy in terms of time efficiency.

6. Conclusion

We have introduced two different reduction relations on monoid semirings: the weak reduction (Section 3) and the strong reduction (Section 4), and we have seen that they both define the congruence that is generated by the underlying set of equations. As the weak reduction is terminating only in very restricted cases, we have considered it in detail only for the special case of free monoid semirings over the natural numbers. For a string rewriting system T on X^*, we have seen that the induced weak reduction relation on $\mathbb{N}X^*$ inherits the termination and confluence properties from the string rewriting relation $\longrightarrow_T$ on X^*, and we have obtained a confluence test for more general systems of the form $T \subset X^* \times \mathbb{N}X^*$ that is based on the notion of critical pairs.

For the strong reduction relation corresponding results have been obtained in less restricted cases. In particular, a confluence test has been derived for finite terminating systems of the form $T \subset X^* \times RX^*$, where R is a commutative semiring.

Finally, we have presented a particular reduction strategy for terminating systems of the form $T \subset X^* \times RX^*$. Based on this reduction strategy the membership problem for the congruence $\Theta(T)$ can be solved algorithmically, if the system T is terminating and confluent, and if the operations on the underlying semiring can be performed effectively.

Now if the given system T is terminating, but not confluent, then those critical pairs $(p, q) \in \mathrm{CP}(T)$ that do not resolve can be interpreted as minimal points of divergence. In the setting of string rewriting systems (in fact, in the more general setting of term rewriting systems) the Knuth–Bendix completion procedure (Knuth and Bendix, 1970) proposes to create additional rules from such critical pairs in order to resolve these divergencies. However, care must be taken in introducing these rules as the resulting system must be guaranteed to still be terminating. As additional rules may result in additional unresolved critical pairs, this process must be iterated. This iteration will result in one of the following three situations:

(1) A finite system $\hat{T}$ is reached for which all critical pairs resolve. Then $\hat{T}$ is convergent, and it is equivalent to T, that is, $\Theta(\hat{T})$ coincides with $\Theta(T)$.
(2) An unresolvable critical pair (p, q) is obtained, from which no rule can be created without destroying the termination property of the actual system. Then one either postpones this pair, hoping that eventually a situation will be reached in which it resolves, or one terminates the procedure with failure.
(3) The iteration does not terminate at all. Then an infinite convergent system $\hat{T}$ is enumerated that is equivalent to T.

Unfortunately, it is not at all clear how this process can be carried over to the reduction relations considered in this paper. If $T \subset X^* \times RX^*$ is a finite terminating system over a commutative semiring R, say, and if T is not confluent, then some of the critical pairs of T do not resolve mod $\Longrightarrow_T$. Unfortunately, as seen in Example 4.20, these critical pairs will in general be polynomials that are not monomials. Thus, they cannot simply be turned into rules of the form (u, q) with $u \in X^*$ and $q \in RX^*$. This means that the technique of the Knuth–Bendix completion procedure carries over to the reduction relations considered here only in very special instances. In order to handle finite and terminating systems of the form $T \subset X^* \times RX^*$ in general, we would need a more general form of reduction relation, a reduction relation that is induced by systems of the form $T' \subset RX^* \times RX^*$. This, however, we have to leave for future work.

For the strong reduction relation considered here, it remains to investigate the confluence property for the case of non-commutative semirings. Further, it remains to consider the confluence property for the situation that the strong reduction relation is not terminating. In that case confluence will in general be undecidable, and therefore sufficient conditions for confluence would be of interest.

Acknowledgements

This work was initiated during a two-month visit of Olga Sokratova at Kassel, which was supported by a grant from the Deutsche Akademischer Austauschdienst (DAAD). She thanks the Department of Mathematics and Computer Science of the University of Kassel for the kind hospitality.

References

Baader, F., Nipkow, T., 1998. Term Rewriting and All That. Cambridge University Press, Cambridge.

Book, R.V., Otto, F., 1993. String-Rewriting Systems. Springer, New York.

DasGupta, B., Sontag, E., 2001. A polynomial-time algorithm for checking equivalence under certain semiring congruences motivated by the state-space isomorphism problem for hybrid systems. Theoret. Comput. Sci. 262, 161–189.

Dershowitz, N., Manna, Z., 1979. Proving termination with multiset orderings. Comm. ACM 22, 465–476.

Gebauer, R., Möller, H.M., 1988. On an installation of Buchberger's algorithm. J. Symbolic Comput. 6, 275–286.

Golan, J.S., 1999. Semirings and Their Applications. Kluwer Academic Publishers, Dordrecht.

Hebisch, U., Weinert, H., 1998. Semirings: Algebraic Theory and Applications in Computer Science. World Scientific Publishing Co., Inc., River Edge, NJ.

Hofbauer, D., 1992. Termination proofs by multiset path orderings imply primitive recursive derivation lengths. Theoret. Comput. Sci. 105, 129–140.

Knuth, D., Bendix, P., 1970. Simple word problems in universal algebras. In: Leech, J. (Ed.), Computational Problems in Abstract Algebra. Pergamon Press, New York, pp. 263–297.

Madlener, K., Reinert, B., 1998a. String rewriting and Gröbner bases—a general approach to monoid and group rings. In: Bronstein, M., Grabmeier, J., Weispfenning, V. (Eds.), Symbolic Rewriting Techniques (Ascona, 1995). Birkhäuser, Basel, pp. 127–180.

Madlener, K., Reinert, B., 1998b. Relating rewriting techniques on monoids and rings: congruences on monoids and ideals in monoid rings. Theoret. Comput. Sci. 208, 3–31.

Mal'cev, A.I., 1954. On general theory of algebraic systems. Mat. Sb. 35, 3–20.

Mora, F., 1985. Gröbner bases for non-commutative polynomial rings. In: Calmet, J. (Ed.), Proceedings AAECC-3. Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science, vol. 229. Springer, Berlin, pp. 353–362.

Pin, J.-E., 1998. Tropical semirings. In: Gunawerdena, J. (Ed.), Idempotency (Bristol 1994). Cambridge University Press, Cambridge, pp. 50–69.

Sokratova, O., 2001. The Mal'cev lemma and rewriting on semirings. Theoret. Comput. Sci. 255, 611–614.