The Knuth-Bendix algorithm and the conjugacy problem in monoids

Fabienne Chouraqui

Abstract We present an algorithmic approach to the conjugacy problem in monoids, using rewriting systems. We extend the classical theory of rewriting developed by Knuth and Bendix to a rewriting that takes into account the cyclic conjugates.

Keywords Rewriting system · Conjugacy problem · Braid monoid

1 Introduction

The use of string rewriting systems or Thue systems has been proved to be a very efficient tool to solve the word problem. Indeed, Book shows that there is a linear-time algorithm to decide the word problem for a monoid that is defined by a finite and complete rewriting system [1]. A question that arises naturally is whether the use of rewriting systems may be an efficient tool for solving other decision problems, specifically the conjugacy problem. Several authors have studied this question, see [8–10], and [11]. The complexity of this question is due to some facts. One point is that for monoids the conjugacy problem and the word problem are independent of each other [10]. This is different from the situation for groups. Another point is that in semigroups and monoids, there are several different notions of conjugacy that are not equivalent in general. We describe them in the following.

Let M be a monoid (or a semigroup) generated by Σ and let u and v be two words in the free monoid Σ^*. The right conjugacy problem asks if there is a word x in the free monoid Σ^* such that $xv =_M ux$, and is denoted by RConj. The left conjugacy problem asks if there is a word y in the free monoid Σ^* such that $vy =_M yu$, and is denoted by LConj. The conjunction of the left and the right conjugacy problems is

F. Chouraqui (✉)
Department of Mathematics, Technion, Haifa, Israel
e-mail: fabienne@techunix.technion.ac.il

denoted by Conj. The relations LConj and RConj are reflexive and transitive but not necessarily symmetric, while Conj is an equivalence relation. A different generalization of conjugacy asks if there are words x, y in the free monoid such that $u =_M xy$ and $v =_M yx$. This is called the *transposition problem* and it is denoted by Trans. This relation is reflexive and symmetric, but not necessarily transitive.

In general, if the answer to this question is positive then the answer to the above questions is also positive, that is Trans $\subseteq$ Conj $\subseteq$ LConj, RConj. For free monoids, Lentin and Schutzenberger show that Trans $=$ Conj $=$ LConj $=$ RConj [6] and for monoids with a special presentation (that is all the relations have the form $r = 1$) Zhang shows that Trans $=$ RConj [15]. We denote by Trans* the transitive closure of Trans. Choffrut shows that Trans* $=$ Conj $=$ LConj $=$ RConj holds in a free inverse monoid *FIM(X)* when restricted to the set of non-idempotents [3]. He shows that LConj is an equivalence relation on *FIM(X)* and he proves the decidability of this problem in this case. Silva generalized the results of Choffrut to a certain class of one-relator inverse monoids. He proves the decidability of Trans for *FIM(X)* with one idempotent relator [12].

In this work, we use rewriting systems in order to solve the conjugacy problems presented above in some semigroups and monoids. A special rewriting system satisfies the condition that all the rules have the form $l \rightarrow 1$, where l is any word. Otto shows that Trans $=$ Conj $=$ LConj for a monoid with a special complete rewriting system and that Trans is an equivalence relation. Moreover, he shows that whenever the rewriting system is finite then the conjugacy problems are solvable [10]. Narendran and Otto show that LConj and Conj are decidable for a finite, length-decreasing and complete rewriting system [8] and that Trans is not decidable [9]. We describe our approach to solve the conjugacy problems using rewriting systems in the following.

Let M be the finitely presented monoid Mon$\langle \Sigma \mid R \rangle$ and let $\Re$ be a complete rewriting system for M. Let u be a word in Σ^*, we consider u and all its cyclic conjugates in Σ^*, $\{u_1 = u, u_2, \ldots, u_k\}$, and we apply on each element u_i rules from $\Re$ (whenever this is possible). We say that a word u is *cyclically irreducible* if u and all its cyclic conjugates are irreducible modulo $\Re$. If for some $1 \leq i \leq n$, u_i reduces to v, then we say that u *cyclically reduces to* v and we denote it by $u \hookrightarrow v$, where $\hookrightarrow$ denotes a binary relation on the words in Σ^*.

We define on $\hookrightarrow$ the properties of terminating and confluent in the same way as for $\rightarrow$ and if $\hookrightarrow$ is terminating and confluent then each word u reduces to a unique cyclically irreducible element denoted by $\rho(u)$. We have the following result that describes the relation between $\hookrightarrow$ and the conjugacy problems, we write $\rho(u) \simeq \rho(v)$ for $\rho(u)$ and $\rho(v)$ are cyclic conjugates in the free monoid Σ^*.

Theorem 1 *Let M be the finitely presented monoid Mon$\langle \Sigma \mid R \rangle$ and let $\Re$ be a complete rewriting system for M. Let u and v be words in Σ^*. Assume that $\hookrightarrow$ is terminating and confluent. Then*

(i) *If u and v are transposed, then $\rho(u) \simeq \rho(v)$.*
(ii) *If $\rho(u) \simeq \rho(v)$, then u and v are left and right conjugates.*

A *completely simple semigroup* is a semigroup that has no non-trivial two-sided ideals and that possesses minimal one-sided ideals. Using the results of McKnight

and Storey in [7], it holds that Trans = Conj in a completely simple semigroup. So, in the case of completely simple semigroups and monoids with a finite special complete rewriting system, our result gives a solution to the conjugacy problems, whenever $\looparrowright$ is terminating and confluent. Assuming that $\looparrowright$ is terminating, we find a sufficient condition for the confluence of $\looparrowright$ that is based on an analysis of the rules in $\Re$. Using this condition, we give an algorithm of cyclical completion that is very much inspired by the Knuth-Bendix algorithm of completion. We have the following main result.

Theorem 2 *Let M be the finitely presented monoid* $\mathrm{Mon}\langle \Sigma \mid R \rangle$ *and let $\Re$ be a complete rewriting system for M. Assume that $\looparrowright$ is terminating. Then there exists an algorithm that gives as an output an equivalent relation $\looparrowright^+$ that is terminating and confluent* (*whenever it converges*).

The paper is organized as follows. In Sect. 2, we define the binary relation $\looparrowright$ on the words in Σ^* and we establish its main properties. In Sect. 3, we describe the connection between a terminating and confluent relation $\looparrowright$ and the conjugacy problems. In Sect. 4, we adopt a local approach as it is very difficult to decide wether a relation $\looparrowright$ is terminating, we define there the notion of triple that is $\tilde{c}$-defined. In Sect. 5, we give a sufficient condition for the confluence of $\looparrowright$, given that it terminates. In Sect. 6, using the results from Sect. 5, we give an algorithm of cyclical completion that is very much inspired by the Knuth-Bendix algorithm of completion. Given a terminating relation $\looparrowright$, if it is not confluent then some new cyclical reductions are added in order to obtain an equivalent relation $\looparrowright^+$ that is terminating and confluent. At last, in Sect. 7, we address the case of length-preserving rewriting systems. All along this paper, $\Re$ denotes a complete rewriting system, not necessarily a finite one.

2 Definition of the relation $\looparrowright$

Let Σ be a non-empty set. We denote by Σ^* the free monoid generated by Σ; elements of Σ^* are finite sequences called *words* and the empty word will be denoted by 1. A *rewriting system* $\Re$ on Σ is a set of ordered pairs in $\Sigma^* \times \Sigma^*$. If $(l, r) \in \Re$ then for any words u and v in Σ^*, we say that the word *ulv reduces* to the word *urv* and we write $ulv \to urv$. A word w is said to be *reducible* if there is a word z such that $w \to z$. If there is no such z we call w *irreducible*. A rewriting system $\Re$ is called *terminating* (*or Noetherian*) if there is no infinite sequence of reductions.

We denote by "$\to^*$" the reflexive transitive closure of the relation "$\to$". A rewriting system $\Re$ is called *confluent* if for any words u, v, w in Σ^*, $w \to^* u$ and $w \to^* v$ implies that there is a word z in Σ^* such that $u \to^* z$ and $v \to^* z$ (that is if u and v have a common ancestor then they have a common descendant). A rewriting system $\Re$ is called *complete* (*or convergent*) if $\Re$ is terminating and confluent. If $\Re$ is complete then every word w in Σ^* has a unique irreducible equivalent word that is called the *normal form* of w. We refer the reader to [2, 13, 14] for more details.

Let $\mathrm{Mon}\langle \Sigma \mid R \rangle$ be a finitely presented monoid M and let $\Re$ be a complete rewriting system for M. Let u and v be elements in Σ^*. We define the following binary relation $u \circlearrowleft^1 v$ if v is a cyclic conjugate of u obtained by moving the first letter of

u to be the last letter of v. We define $u \circlearrowleft^i v$ if v is a cyclic conjugate of u obtained from i successive applications of $\circlearrowleft^1$. We allow i being 0 and in this case if $u \circlearrowleft^0 v$ then $v = u$ in the free monoid Σ^*. As an example, let u be the word *abcdef* in Σ^*. If $u \circlearrowleft^1 v$ and $u \circlearrowleft^4 w$, then v is the word *bcdefa* and w is the word *efabcd* in Σ^*.

We now translate the operation of taking cyclic conjugates and reducing them using the rewriting system $\Re$ in terms of a binary relation. We say that u *cyclically reduces to* v and we write

$$u \rightsquigarrow v \tag{2.1}$$

if there is a sequence

$$u \circlearrowleft^i \tilde{u} \rightarrow v \tag{2.2}$$

From its definition, the relation $\rightsquigarrow$ is *not* compatible with concatenation. We define by $\rightsquigarrow^*$ the reflexive and transitive closure of $\rightsquigarrow$, that is $u \rightsquigarrow^* v$ if there is a sequence $u \rightsquigarrow u_1 \rightsquigarrow u_2 \rightsquigarrow \ldots u_{k-1} \rightsquigarrow v$. We call such a sequence *a sequence of cyclical reductions*. A sequence of cyclical reductions is *trivial* if it is equivalent to $\circlearrowleft^*$. We use the following notation:

- $\tilde{u}$ denotes a cyclic conjugate of u in the free monoid Σ^*.
- $u \simeq v$ if u and v are cyclic conjugates in the free monoid Σ^*.
- $u =_M v$ if the words u and v are equal as elements in M.
- $u = v$ if the words u and v are equal in the free monoid Σ^*.

Now, we define the properties of terminating and confluent for $\rightsquigarrow$ in the same way as it is done for $\rightarrow$. Note that given words u and v if we write $u \rightsquigarrow v$ or $u \rightsquigarrow^* v$, we assume implicitly that this is done in a finite number of steps.

Definition 2.1 We say that $\Re$ is *cyclically terminating* (or $\rightsquigarrow$ is *terminating*) if there is no (non-trivial) infinite sequence of cyclical reductions. We say that $\Re$ is *cyclically confluent* (or $\rightsquigarrow$ is *confluent*) if for any words u, v, w in Σ^*, $w \rightsquigarrow^* u$ and $w \rightsquigarrow^* v$ implies that there exist cyclically conjugates words z and z' in Σ^* such that $u \rightsquigarrow^* z$ and $v \rightsquigarrow^* z'$. We say that $\Re$ is *locally cyclically confluent* (or $\rightsquigarrow$ is *locally confluent*) if for any words u, v, w in Σ^*, $w \rightsquigarrow u$ and $w \rightsquigarrow v$ implies that there exist cyclically conjugates words z and z' in Σ^* such that $u \rightsquigarrow^* z$ and $v \rightsquigarrow^* z'$. We say that $\Re$ is *cyclically complete* if $\Re$ is cyclically terminating and cyclically confluent.

Example 2.2 Let $\Re = \{ab \rightarrow bc, cd \rightarrow da\}$, $\Re$ is a complete and finite rewriting system. Consider the word *bcd*, we have $bcd \rightarrow bda \circlearrowleft^2 abd \rightarrow bcd \rightarrow \ldots$, that is there is an infinite sequence of cyclical reductions. So, $\Re$ is not cyclically terminating.

Definition 2.3 We say that a word u is *cyclically irreducible* if u and all its cyclic conjugates are irreducible modulo $\Re$, that is there is no v in Σ^* such that $u \rightsquigarrow v$ (unless $u \simeq v$). We define a *cyclically irreducible form of u* (if it exists) to be a cyclically irreducible word v (up to $\simeq$) such that $u \rightsquigarrow^* v$. We denote by $\rho(u)$ a cyclically irreducible form of u, if it exists.

Example 2.4 Let $\Re = \{ab \to bc, cd \to da\}$ as before. From Example 2.2, *bcd* does not have any cyclically irreducible form. But, the word *acd* has a unique cyclically irreducible form *ada* since $acd \to ada$ and no rule from $\Re$ can be applied on *ada* or on any cyclic conjugate of *ada* in Σ^*.

As in the case of $\to$, the following facts hold also for $\looparrowright$ with a very similar proof. If $\Re$ is cyclically terminating, then each word in Σ^* has at least one cyclically irreducible form. If $\Re$ is cyclically confluent, then each word in Σ^* has at most one cyclically irreducible form. So, if $\Re$ is cyclically complete, then each word in Σ^* has a unique cyclically irreducible form. Moreover, if $w \simeq w'$, then w and w' have the same cyclically irreducible form (up to $\simeq$). Given that $\looparrowright$ is terminating, $\Re$ is cyclically confluent if and only if $\Re$ is locally cyclically confluent.

Example 2.5 In [5], Hermiller and Meier construct a finite and complete rewriting system for the group $\mathrm{Gp}\langle a, b \mid aba = bab\rangle$, using another set of generators. For the monoid with the same presentation, the set of generators is: $\{a, b, \underline{ab}, \underline{ba}, \Delta = \underline{aba}\}$, where the underlining of a sequence of letters means that it is a generator in the new generating set. The complete and finite rewriting system is $\Re = \{ab \to \underline{ab}, ba \to \underline{ba}, a\underline{ba} \to \Delta, \underline{ab}a \to \Delta, bab \to \Delta, \underline{ab}\,\underline{ab} \to a\Delta, \underline{bab} \to \Delta, \underline{ba}\,\underline{ba} \to b\Delta, \Delta a \to b\Delta, \Delta b \to a\Delta, \Delta\underline{ab} \to \underline{ba}\Delta, \Delta\underline{ba} \to \underline{ab}\Delta\}$. Let consider the word *ab*, then $ab \to \underline{ab}$ and $ab \circlearrowleft^1 ba \to \underline{ba}$. That is, $ab \looparrowright \underline{ab}$ and $ab \looparrowright \underline{ba}$, where both $\underline{ab}$ and $\underline{ba}$ are cyclically irreducible, so $\Re$ is not cyclically confluent (nor locally cyclically confluent).

3 The relation $\looparrowright$ and the conjugacy problems

We denote by $u \equiv_M v$ the following equivalence relation: there are words x, y in Σ^* such that $ux =_M xv$ and $yu =_M vy$, that is u and v are left and right conjugates. We describe the connection between the relations $\looparrowright$, $\equiv$ and the transposition problem.

Proposition 3.1 *Let M denote the finitely presented monoid $\mathrm{Mon}\langle \Sigma \mid R \rangle$ and let $\Re$ be a complete rewriting system for M. Let u and v be in Σ^*.*

(i) *If $u \looparrowright^* v$, then the pair (u, v) is in the transitive closure of the transposition relation and therefore $u \equiv_M v$.*
(ii) *If $\rho(u) \simeq \rho(v)$, then $u \equiv_M v$ (whenever $\rho(u)$ and $\rho(v)$ exist).*

Proof (i) If the sequence of cyclical reductions has the following form: $u \circlearrowleft^i \tilde{u} \to^* v$, then u and v are transposed. Otherwise, if $u = u_1 \circlearrowleft^i \tilde{u} \to^* u_2 \circlearrowleft^i \tilde{u}_2 \to^* u_3 \ldots \to^* u_k = v$, then each pair (u_i, u_{i+1}) is transposed. So, the pair (u, v) is in the transitive closure of the transposition relation and therefore $u \equiv_M v$. (ii) From (i), $u \equiv_M \rho(u)$ and $v \equiv_M \rho(v)$, so $u \equiv_M v$, since $\rho(u) \simeq \rho(v)$ and $\equiv_M$ is an equivalence relation. $\square$

The converse of (ii) is not true in general, namely $u \equiv_M v$ does not imply that $\rho(u) \simeq \rho(v)$. Let $\Re = \{bab \to aba, ba^n ba \to aba^2 b^{n-1}, n \geq 2\}$. Then $\Re$ is a complete and infinite rewriting system for the braid monoid presented by $\mathrm{Mon}\langle a, b \mid$

$aba = bab\rangle$. It holds that $a \equiv_M b$, since $a(aba) =_M (aba)b$ and $(aba)a =_M b(aba)$, but $\rho(a) = a$ and $\rho(b) = b$ and they are not cyclic conjugates. This example is due to Patrick Dehornoy.

Lemma 3.2 *Let $\mathfrak{R}$ be a complete and cyclically complete rewriting system for M. Let u and v be words in Σ^*. If $u =_M v$, then $\rho(u) \simeq \rho(v)$.*

Proof Assume that $u \looparrowright^* z$ and $v \looparrowright^* z'$, where z, z' are cyclically irreducible. We show that $z \simeq z'$. Since $\mathfrak{R}$ is a complete rewriting system, equivalent words (modulo $\mathfrak{R}$) reduce to the same normal form. Here $u =_M v$, so there is a unique irreducible word w such that $u \to^* w$ and $v \to^* w$.

We have the following diagram:

$$
\begin{array}{c}
u \looparrowright^* z \\
\searrow{}^* \\
w \\
\nearrow{}^* \\
v \looparrowright^* z'
\end{array}
$$
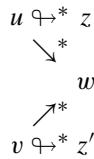
Assume that $w \looparrowright^* z''$, so $u \looparrowright^* z''$ and $v \looparrowright^* z''$. But $u \looparrowright^* z$ and $v \looparrowright^* z'$ and $\mathfrak{R}$ is cyclically complete, so $z \simeq z'' \simeq z'$. $\square$

Theorem 3.3 *Let $\mathfrak{R}$ be a complete and cyclically complete rewriting system for M. Let u and v be words in Σ^*.*

(i) *If u and v are transposed, then $\rho(u) \simeq \rho(v)$.*
(ii) *If $\rho(u) \simeq \rho(v)$, then $u \equiv_M v$.*

Proof (i) Since u and v are transposed, there are words x and y in Σ^* such that $u =_M xy$ and $v =_M yx$. From Lemma 3.2, $\rho(xy) \simeq \rho(u)$ and $\rho(yx) \simeq \rho(v)$. Moreover, since $xy \simeq yx$ and $\mathfrak{R}$ is cyclically complete, $\rho(xy) \simeq \rho(yx)$, so $\rho(u) \simeq \rho(v)$.
(ii) holds from Proposition 3.1 in a more general context. $\square$

4 A local approach for $\looparrowright$: definition of Allseq(w)

Given a complete rewriting system $\mathfrak{R}$, it is a very hard task to determine if $\mathfrak{R}$ is cyclically terminating, since we have to check a potentially infinite number of words. So, we adopt a local approach, that is for each word w in Σ^* we consider all the possible sequences of cyclical reductions that begin by each word from $\{w_1, \ldots, w_k\}$, where $w_1 = w, w_2, \ldots, w_k$ are all the cyclic conjugates of w in Σ^*. We call the set of all these sequences Allseq(w). We say that Allseq(w) *terminates* if there is no infinite sequence of cyclical reductions in Allseq(w). Clearly, $\mathfrak{R}$ is cyclically terminating if and only if Allseq(w) terminates for every w in Σ^*.

Example 4.1 Let $\mathfrak{R} = \{bab \to aba, ba^n ba \to aba^2 b^{n-1}$, where $n \geq 2\}$. Then $\mathfrak{R}$ is a complete and infinite rewriting system for the braid monoid presented by $\mathrm{Mon}\langle a, b \mid$

$aba = bab$⟩. We denote by w the word ba^2ba. We have the following infinite sequence of cyclical reductions: $ba^2ba \rightarrow aba^2b \circlearrowleft^1 ba^2ba$, that is $\mathrm{Allseq}(w)$ does not terminate. This holds also for ba^nba for each $n \geq 2$.

We say that $\mathrm{Allseq}(w)$ *converges* if a unique cyclically irreducible form is achieved in $\mathrm{Allseq}(w)$ (up to $\simeq$). Clearly, if $\Re$ is cyclically confluent then $\mathrm{Allseq}(w)$ converges for every w in Σ^*. The converse is true only if $\Re$ is cyclically terminating. We illustrate this with an example.

Example 4.2 Let $\Re = \{bab \rightarrow aba, ba^nba \rightarrow aba^2b^{n-1}$, where $n \geq 2\}$ as in Example 4.1. It holds that $\mathrm{Allseq}(ba^2ba)$ does not terminate (see Example 4.1). Yet, $\mathrm{Allseq}(ba^2ba)$ converges, since a^3ba is the unique cyclically irreducible form achieved in $\mathrm{Allseq}(w)$. Indeed, there is the following sequence of cyclical reductions: $ba^2ba \circlearrowleft^1 a^2bab \rightarrow a^3ba$ and all the cyclic conjugates of w cyclically reduce to a^3ba. So, although $\mathrm{Allseq}(ba^2ba)$ does not terminate, a unique cyclically irreducible form a^3ba is achieved.

We find a condition that ensures that $\mathrm{Allseq}(w)$ converges, given that $\mathrm{Allseq}(w)$ terminates. Before we proceed, we give the following definition.

Definition 4.3 Let $\Re$ be a complete rewriting system and let w be a word in Σ^*. Let r_1 and r_2 be rules in $\Re$ such that r_1 can be applied on a cyclic conjugate of w and r_2 can be applied on another one. We say that *the triple* (w, r_1, r_2) *is $\tilde{c}$-defined* if there is a cyclic conjugate $\tilde{w}$ of w such that both rules r_1 and r_2 can be applied on $\tilde{w}$. We allow an empty entry in a triple (w, r_1, r_2), that is only r_1 or r_2 can be applied.

Example 4.4 Let $\mathrm{Mon}\langle x, y, z \mid xy = yz = zx \rangle$, this is the Wirtinger presentation of the trefoil knot group. Let $\Re = \{xy \rightarrow zx, yz \rightarrow zx, xz^nx \rightarrow zxzy^{n-1}, n \geq 1\}$ be a complete and infinite rewriting system for the monoid with this presentation (see [4]). Let consider the word yxz^2x, yxz^2x and $xyxz^2$ are cyclic conjugates on which the rules $xz^2x \rightarrow zxzy$ and $xy \rightarrow zx$ can be applied respectively. We claim that the triple $(yxz^2x, xz^2x \rightarrow zxzy, xy \rightarrow zx)$ is $\tilde{c}$-defined. Indeed, there is the cyclic conjugate xz^2xy on which both the rules $xz^2x \rightarrow zxzy$ and $xy \rightarrow zx$ can be applied. But, as an example the triple $(xz^2xz^3, xz^2x \rightarrow zxzy, xz^3x \rightarrow zxzy^2)$ is not $\tilde{c}$-defined.

In what follows, we show that if $\mathrm{Allseq}(w)$ terminates and all the triples occurring there are $\tilde{c}$-defined, then $\mathrm{Allseq}(w)$ converges. The following lemma is the induction basis of the proof. For brevity, we write $u \looparrowright^{r_1} v_1$ for $u \circlearrowleft u_1 \rightarrow^{r_1} v_1$, where $u_1 \rightarrow^{r_1} v_1$ means that v_1 is obtained from the application of the rule r_1 on u_1.

Lemma 4.5 *Let the triple* (w, r_1, r_2) *be $\tilde{c}$-defined. Assume that $w \looparrowright^{r_1} v_1$ and $w \looparrowright^{r_2} v_2$, then there are cyclically conjugates words z_1 and z_2 such that $v_1 \looparrowright^* z_1$ and $v_2 \looparrowright^* z_2$.*

Proof We denote by ℓ_1 and ℓ_2 the left-hand sides of the rules r_1 and r_2 respectively and by m_1 and m_2 the corresponding right-hand sides. Then ℓ_1 has an occurrence

in w_1 and ℓ_2 has an occurrence in w_2, where $w_1 \simeq w_2 \simeq w$. Since (w, r_1, r_2) is $\tilde{c}$-defined, there exists $\tilde{w}$ such that $\tilde{w} \simeq w$ and ℓ_1 and ℓ_2 both have an occurrence in $\tilde{w}$. Then one of the following holds:

(i) $\tilde{w} = x\ell_1 y\ell_2 s$, where x, y, s are words.
(ii) $\tilde{w} = x\ell_2 y\ell_1 s$, where x, y, s are words.
(iii) $\tilde{w} = x\ell_1 \ell_2'' y$, where x, y are words, $\ell_1 = \ell_1'\ell_1''$, $\ell_2 = \ell_2'\ell_2''$ and $\ell_1'' = \ell_2'$.
(iv) $\tilde{w} = x\ell_2 \ell_1'' y$, where x, y are words, $\ell_1 = \ell_1'\ell_1''$, $\ell_2 = \ell_2'\ell_2''$ and $\ell_2'' = \ell_1'$.
(v) $\tilde{w} = x\ell_2 y$, where x, y are words, ℓ_1 is a subword of ℓ_2.
(vi) $\tilde{w} = x\ell_1 y$, where x, y are words, ℓ_2 is a subword of ℓ_1.

We check the cases (i), (iii) and (v) and the other three cases are symmetric. If both ℓ_1 and ℓ_2 have an occurrence in w_1 and in w_2, then obviously there are words z_1 and z_2 such that $v_1 \looparrowright z_1$ and $v_2 \looparrowright z_2$, where $z_1 \simeq z_2$. So, assume that ℓ_1 has no occurrence in w_2 and ℓ_2 has no occurrence in w_1.

Case (i): Assume that $\tilde{w} = x\ell_1 y\ell_2 s$. Then the words w_1 and w_2 have the following form: $w_1 = \ell_2'' sx\ell_1 y\ell_2'$ and $w_2 = \ell_1'' y\ell_2 sx\ell_1'$, where $\ell_1 = \ell_1'\ell_1''$ and $\ell_2 = \ell_2'\ell_2''$. This is due to the fact that ℓ_1 has no occurrence in w_2 and ℓ_2 has no occurrence in w_1. So, $w_1 = \ell_2'' sx\ell_1 y\ell_2' \to \ell_2'' sxm_1 y\ell_2' \circlearrowleft^i sxm_1 y\ell_2'\ell_2'' \to sxm_1 ym_2$ and $w_2 = \ell_1'' y\ell_2 sx\ell_1' \to \ell_1'' ym_2 sx\ell_1' \circlearrowleft^j ym_2 sx\ell_1'\ell_1'' \to ym_2 sxm_1$. We take then z_1 to be $sxm_1 ym_2$ and z_2 to be $ym_2 sxm_1$.

Case (iii): Assume that $\tilde{w} = x\ell_1 \ell_2'' y$, where $\ell_1'' = \ell_2'$. There is an overlap ambiguity between these rules which resolve, since $\mathfrak{R}$ is complete:

$$\ell_1'\ell_1''\ell_2''$$
$$m_1\ell_2'' \swarrow \qquad \searrow \ell_1' m_2$$
$$\searrow^* \qquad \qquad \swarrow^*$$
$$z$$
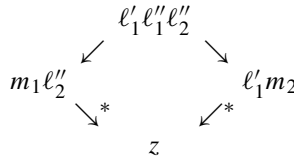
The words w_1 and w_2 have the following form: $w_1 = \ell_2'' yx\ell_1$ and $w_2 = \ell_2 yx\ell_1'$. So, $w_1 = \ell_2'' yx\ell_1 \to \ell_2'' yxm_1 \circlearrowleft^i m_1\ell_2'' yx \to^* zyx$ and $w_2 = \ell_2 yx\ell_1' \to m_2 yx\ell_1' \circlearrowleft^j \ell_1' m_2 yx \to^* zyx$. So, we take z_1 and z_2 to be zyx.

Case (v): Assume that $\tilde{w} = x\ell_2 y$, where $\ell_2 = s\ell_1 t$. There is an inclusion ambiguity between these rules which resolve, since $\mathfrak{R}$ is complete:

$$\ell_2 = s\ell_1 t$$
$$sm_1 t \swarrow \qquad \searrow m_2$$
$$\searrow^* \qquad \qquad \swarrow^*$$
$$z$$
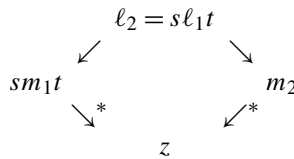
The words w_1 and w_2 have the following form: $w_1 = tyxs\ell_1$ and $w_2 = \tilde{w} = x\ell_2 y$. So, $w_1 = tyxs\ell_1 \to tyxsm_1 \circlearrowleft^i sm_1 tyx \to^* zyx$ and $w_2 = x\ell_2 y \to xm_2 y \to^* xzy$. So, we take z_1 to be zyx and z_2 to be xzy. $\square$

Proposition 4.1 *Let w be a word in Σ^* and assume that* Allseq(w) *terminates. Assume all the triples in* Allseq(w) *are $\tilde{c}$-defined, then* Allseq(w) *converges.*

Proof We show that the restriction of $\looparrowright$ to Allseq(w) is confluent. Since Allseq(w) terminates, it is enough to show that the restriction of $\looparrowright$ to Allseq(w) is locally confluent. All the triples in Allseq(w) are $\tilde{c}$-defined, so from Lemma 4.5 the restriction of $\looparrowright$ to Allseq(w) is locally confluent. $\qquad\square$

5 A sufficient condition for the confluence of $\looparrowright$

We find a sufficient condition for the confluence of $\looparrowright$, that is based on an analysis of the rules in $\mathfrak{R}$. For that, we translate the signification of a triple that is not $\tilde{c}$-defined in terms of the rules in $\mathfrak{R}$.

Definition 5.1 Let $w = x_1 x_2 x_3 \cdots x_k$ be a word, where the x_i are generators for $1 \leq i \leq k$. Then we define the following sets of words:

$$\mathrm{pre}(w) = \{x_1, x_1 x_2, x_1 x_2 x_3, \ldots, x_1 x_2 x_3 \ldots x_k\}$$

$$\mathrm{suf}(w) = \{x_k, x_{k-1} x_k, x_{k-2} x_{k-1} x_k, \ldots, x_1 x_2 x_3 \ldots x_k\}$$

Lemma 5.2 *Let (w, r_1, r_2) be a triple and let ℓ_1 and ℓ_2 denote the left-hand sides of the rules r_1 and r_2, respectively. If $\mathrm{pre}(\ell_2) \cap \mathrm{suf}(\ell_1) = \emptyset$ or $\mathrm{pre}(\ell_1) \cap \mathrm{suf}(\ell_2) = \emptyset$, then the triple (w, r_1, r_2) is $\tilde{c}$-defined.*

Proof From the assumption, ℓ_1 is a subword of w_1 and ℓ_2 is a subword of w_2, where w_1 and w_2 are cyclic conjugates of w. We show that there exists a cyclic conjugate of w, $\tilde{w}$, such that both ℓ_1 and ℓ_2 are subwords of $\tilde{w}$. If $\mathrm{pre}(\ell_2) \cap \mathrm{suf}(\ell_1) = \emptyset$ and $\mathrm{pre}(\ell_1) \cap \mathrm{suf}(\ell_2) = \emptyset$ or if $\mathrm{pre}(\ell_2) \cap \mathrm{suf}(\ell_1) \neq \emptyset$ and $\mathrm{pre}(\ell_1) \cap \mathrm{suf}(\ell_2) = \emptyset$, take $\tilde{w}$ to be such that it ends in ℓ_2 and then ℓ_1 will also have an occurrence in $\tilde{w}$. If $\mathrm{pre}(\ell_2) \cap \mathrm{suf}(\ell_1) = \emptyset$ and $\mathrm{pre}(\ell_1) \cap \mathrm{suf}(\ell_2) \neq \emptyset$, take $\tilde{w}$ to be such that it ends in ℓ_1 and then ℓ_2 will also have an occurrence in $\tilde{w}$. $\qquad\square$

Note that if $\mathrm{pre}(\ell_2) \cap \mathrm{suf}(\ell_1) \neq \emptyset$ and $\mathrm{pre}(\ell_1) \cap \mathrm{suf}(\ell_2) \neq \emptyset$, then it does not necessarily imply that all the triples of the form (w, r_1, r_2) are not $\tilde{c}$-defined. Yet, as the following example illustrates it, there exists a triple (w, r_1, r_2) that is not $\tilde{c}$-defined.

Example 5.3 Let $\mathfrak{R} = \{xy \to zx, yz \to zx, xz^n x \to zxzy^{n-1}, n \geq 1\}$ from Example 4.4. The rules $xz^2 x \to zxzy$ and $xz^3 x \to zxzy^2$ satisfy $\mathrm{pre}(xz^2 x) \cap \mathrm{suf}(xz^3 x) = \{x\}$ and $\mathrm{pre}(xz^3 x) \cap \mathrm{suf}(xz^2 x) = \{x\}$. Yet, the triple $(xz^2 xz^3 x, xz^2 x \to zxzy, xz^3 x \to zxzy^2)$ is $\tilde{c}$-defined, but the triple $(xz^2 xz^3, xz^2 x \to zxzy, xz^3 x \to zxzy^2)$ is not $\tilde{c}$-defined.

Lemma 5.4 *Let (w, r_1, r_2) be a triple and we denote by ℓ_1 and ℓ_2 the left-hand sides of the rules r_1 and r_2, respectively. Assume that (w, r_1, r_2) is not $\tilde{c}$-defined. Then $\ell_1 = xuy$ and $\ell_2 = yvx$, where u, v are words and x, y are non-empty words.*

Proof The triple (w, r_1, r_2) is not $\tilde{c}$-defined, so from Lemma 5.2, $\mathrm{pre}(\ell_2) \cap \mathrm{suf}(\ell_1) \neq \emptyset$ and $\mathrm{pre}(\ell_1) \cap \mathrm{suf}(\ell_2) \neq \emptyset$. Assume that $\mathrm{pre}(\ell_2) \cap \mathrm{suf}(\ell_1) \supseteq \{x\}$ and $\mathrm{pre}(\ell_1) \cap \mathrm{suf}(\ell_2) \supseteq \{y\}$, where x, y are non-empty words. So, ℓ_1 and ℓ_2 have one of the following forms:

   (i) $\ell_1 = xuy$ and $\ell_2 = yvx$, where u, v are words.
   (ii) $\ell_1 = xy$ and $\ell_2 = yx''$, where $x = x'x''$, $y = y'y''$ and $y'' = x'$.
   (iii) $\ell_1 = xy''$ and $\ell_2 = yx$, where $x = x'x''$, $y = y'y''$ and $x'' = y'$.
   (iv) $\ell_1 = xy''$ and $\ell_2 = yx''$, where $x = x'x''$, $y = y'y''$, and $y'' = x'$, $x'' = y'$.

We show that only case (i) occurs, by showing that in the cases (ii), (iii) and (iv) the triple (w, r_1, r_2) is $\tilde{c}$-defined. This is done by describing $\tilde{w}$ on which both r_1 and r_2 can be applied. In any case, w_1 has to contain an occurrence of ℓ_1 and w_2 has to contain an occurrence of ℓ_2, where w_1 and w_2 are cyclic conjugates of w. In case (ii), $\ell_1 = x'x''y'y''$ and $\ell_2 = y'y''x''$, where $y'' = x'$, so there exists $\tilde{w} = x'x''y'y''x''$ that contains an occurrence of ℓ_1 and an occurrence of ℓ_2. Case (iii) is symmetric to case (ii) and we consider case (iv). In case (iv), $\ell_1 = x'x''y''$ and $\ell_2 = y'y''x''$, where $y'' = x'$ and $x'' = y'$, so using the same argument as before, take $\tilde{w}$ to be $x'x''y''x''$. So, case (i) occurs and w has the form $xuyv$.   □

Definition 5.5 We say that there is a *cyclical overlap* between rules, if there are two rules in $\Re$ of the form $xuy \to u'$ and $yvx \to v'$, where u', v' are words, u, v, x, y are non-empty words and such that $u'v$ and $v'u$ are not cyclic conjugates in Σ^*. We say that there is a *cyclical inclusion* if there are two rules in $\Re$, $l \to v$ and $l' \to v'$, where l, v, l', v' are words and l' is a cyclic conjugate of l or l' is a proper subword of a cyclic conjugate of l. Whenever l' is a cyclic conjugate of l, v and v' are not cyclic conjugates in Σ^* and whenever l' is a proper subword of ℓ_1, where ℓ_1 is a cyclic conjugate of l (there is a non-empty word u such that $\ell_1 = ul'$), then it holds that $l \to r$ and $l \circlearrowright^i \ell_1 = ul' \to uv'$ and v and uv' are not cyclic conjugates in Σ^*.

In Example 5.3, there is a cyclical overlap between the rules $xz^2x \to zxzy$ and $xz^3x \to zxzy^2$. In Example 2.5, there is a cyclical inclusion between the rules $ab \to \underline{ab}$ and $ba \to \underline{ba}$, since ab is a cyclic conjugate of ba. In Example 4.1, there is a cyclical inclusion of the rule $bab \to aba$ in the rule $ba^2ba \to aba^2b$, since bab is a subword of $baba^2$ (a cyclic conjugate of ba^2ba).

Lemma 5.6 *Let (w, r_1, r_2) be a triple and let ℓ_1 and ℓ_2 be the left-hand sides of the rules r_1 and r_2, respectively. Assume that the triple (w, r_1, r_2) is not $\tilde{c}$-defined. Then there is a cyclical overlap or a cyclical inclusion between r_1 and r_2.*

Proof The triple (w, r_1, r_2) is not $\tilde{c}$-defined, so from Lemma 5.4, $\ell_1 = xuy$ and $\ell_2 = yvx$, where x, y are non-empty words and u, v are words. If u and v are both the empty word, then ℓ_1 and ℓ_2 are cyclic conjugates, that is there is a cyclical inclusion. If u is the empty word but v is not the empty word, then $\ell_1 = xy$ and $\ell_2 = yvx$, which means that ℓ_1 is a subword of a cyclic conjugate of ℓ_2. So, in this case and in the symmetric case (that is v is the empty word but u is not the empty word) there is a cyclical inclusion. If none of u and v is the empty word, then $\ell_1 = xuy$ and $\ell_2 = yvx$, that is there is a cyclical overlap between these two rules.   □

Proposition 5.7 *Let w be a word in Σ^* and assume that* Allseq(w) *terminates. If there are no cyclical overlaps and cyclical inclusions in* Allseq(w), *then* Allseq(w) *converges.*

Proof If Allseq(w) does not converge, then from Proposition 4.1, this implies that there is a triple (w, r_1, r_2) in Allseq(w) that is not $\tilde{c}$-defined. From Lemma 5.6, this implies that there is a cyclical overlap or a cyclical inclusion in Allseq(w). □

Note that the converse is not necessarily true, that is there may be a cyclical overlap or a cyclical inclusion in Allseq(w) and yet a unique cyclically irreducible form is achieved in Allseq(w), as in the following example.

Example 5.8 Let $\Re = \{bab \rightarrow aba, ba^n ba \rightarrow aba^2 b^{n-1}, n \geq 2\}$. Let $w = ba^2 ba$, then Allseq(w) does not terminate (see Example 4.1). The triple $(w, bab \rightarrow aba, ba^2 ba \rightarrow aba^2 b)$ is not $\tilde{c}$-defined since there is a cyclical inclusion of the rule $bab \rightarrow aba$ in the rule $ba^2 ba \rightarrow aba^2 b$. Nevertheless, w has a unique cyclically irreducible form ba^4 (up to $\simeq$): $ba^2 ba \rightarrow aba^2 b \circlearrowleft^4 baba^2 \rightarrow abaa^2$. In fact, each $w = ba^n ba$ where $n \geq 2$ has a unique cyclically irreducible form ba^{n+2} (up to $\simeq$).

Theorem 5.9 *Let $\Re$ be a complete rewriting system that is cyclically terminating. If there are no rules in $\Re$ with cyclical overlaps or cyclical inclusions, then $\Re$ is cyclically confluent.*

Proof From Proposition 5.7, if there are no rules in $\Re$ with cyclical overlaps or cyclical inclusions then Allseq(w) converges for all w. Since $\Re$ is cyclically terminating, $\Re$ is cyclically confluent if and only if Allseq(w) converges for all w, so the proof is done. □

6 The algorithm of cyclical completion

Knuth and Bendix have elaborated an algorithm which for a given finite and terminating rewriting system $\Re$, tests its completeness and if $\Re$ is not complete then new rules are added to complete it. This procedure can have one of three outcomes: success in finding a finite and complete system, failure in finding anything or looping and generating an infinite number of rules (see [14]). Instead of testing the confluence of $\Re$, the algorithm tests the locally confluence of $\Re$, since for a terminating rewriting system locally confluence and confluence are equivalent. Two rewriting systems $\Re$ and $\Re'$ are said to be *equivalent* if: $w_1 \leftrightarrow^* w_2$ modulo $\Re$ if and only if $w_1 \leftrightarrow^* w_2$ modulo $\Re'$. So, by applying the Knuth-Bendix algorithm on a terminating rewriting system $\Re$ a complete rewriting system $\Re'$ that is equivalent to $\Re$ can be found (if the algorithm does not fail). Our aim in this section is to provide an algorithm of cyclical completion which is much inspired by the Knuth-Bendix algorithm of completion.

Let $\Re$ be a complete and cyclically terminating rewriting system, we assume that $\Re$ is finite. From Theorem 5.9, if there are no cyclical overlaps or cyclical inclusions then $\Re$ is cyclically confluent. Nevertheless, if there is a cyclical overlap or a cyclical

inclusion, we define when it resolves in the following way. We say that the cyclical overlap between the rules $xuy \to u'$ and $yvx \to v'$, where u, v, u', v' are words, x, y are non-empty words *resolves* if there exist cyclically conjugate words z and z' such that $u'v \leftrightsquigarrow^* z$ and $uv' \leftrightsquigarrow^* z'$. If there is a cyclical inclusion between the rules $l \to v$ and $l' \to v'$, where l, v, l', v' are words and l' is a cyclic conjugate of l or l' is a proper subword of a cyclic conjugate of l, then we say that it resolves if there exist cyclically conjugate words z and z' such that $v \leftrightsquigarrow^* z$ and $v' \leftrightsquigarrow^* z'$ in the first case or $v \leftrightsquigarrow^* z$ and $uv' \leftrightsquigarrow^* z'$ in the second case ($z \simeq z'$).

Example 6.1 We consider the complete and finite rewriting system from Example 2.5. Since there is a cyclical inclusion between the rules $ab \to \underline{ab}$ and $ba \to \underline{ba}$, it holds that $ab \leftrightsquigarrow \underline{ab}$ and $ab \leftrightsquigarrow \underline{ba}$, where $\underline{ab}$ and $\underline{ba}$ are cyclically irreducible. We can decide arbitrarily wether $\underline{ab} \leftrightsquigarrow^+ \underline{ba}$ or $\underline{ba} \leftrightsquigarrow^+ \underline{ab}$, in any case this cyclical inclusion resolves.

In the following, we describe the algorithm of cyclical completion in which we add some new cyclical reductions. We denote by $\mathfrak{R}^+$ the rewriting system with the added cyclical reductions and we add "+" in $\leftrightsquigarrow^+$ for each cyclical reduction that is added in the process of cyclical completion. We assume that $\mathfrak{R}$ is a finite, complete and cyclically terminating rewriting system. The algorithm is described in the following.

(i) If there are no cyclical overlaps or cyclical inclusions, then $\mathfrak{R}$ is cyclically confluent, from Theorem 5.9 and $\mathfrak{R}^+ = \mathfrak{R}$.
(ii) Assume there is a cyclical overlap or a cyclical inclusion in the word w: $w \leftrightsquigarrow z_1$ and $w \leftrightsquigarrow z_2$.

With no loss of generality, we can assume that z_1 and z_2 are cyclically irreducible (since otherwise we can first cyclically reduce them), then decide $z_1 \leftrightsquigarrow^+ z_2$ or $z_2 \leftrightsquigarrow^+ z_1$. If at a former step, no $z_i \leftrightsquigarrow^+ u$ or $u \leftrightsquigarrow^+ z_i$ for $i = 1, 2$ was added, then we can decide arbitrarily wether $z_1 \leftrightsquigarrow^+ z_2$ or $z_2 \leftrightsquigarrow^+ z_1$. As an example, if $z_1 \leftrightsquigarrow^+ u$ was added, then we choose $z_2 \leftrightsquigarrow^+ z_1$.

The algorithm fails if the addition of a new cyclical reduction creates a contradiction: assume z_1 and z_2 are cyclically irreducible and we need to add $z_1 \leftrightsquigarrow^+ z_2$ or $z_2 \leftrightsquigarrow^+ z_1$ but $z_1 \leftrightsquigarrow^+ u$ and $z_2 \leftrightsquigarrow^+ v$ are already in $\mathfrak{R}^+$. In the Knuth-Bendix algorithm of completion, the addition of the new rules may create some additional overlap or inclusion ambiguities. We show in the following that this is not the case with the algorithm of cyclical completion and this is due to the fact that the relation $\leftrightsquigarrow$ is not compatible with concatenation. From Proposition 3.1, if $u \leftrightsquigarrow^* v$ then $u \equiv_M v$. In the following lemma, we show that this holds also with $\leftrightsquigarrow^+$.

Lemma 6.2 *Let $\mathfrak{R}$ be a complete and cyclically terminating rewriting system. We assume that $\mathfrak{R}$ is finite. Let $\mathfrak{R}^+$ be the cyclical rewriting system obtained from the application of the algorithm of cyclical completion on $\mathfrak{R}$. If $u \leftrightsquigarrow^+ v$ then $u \equiv_M v$ modulo $\mathfrak{R}$.*

Proof There are two cases to check: if $u \leftrightsquigarrow^+ v$ and if $u \leftrightsquigarrow^+ u_2 \leftrightsquigarrow^+ u_3 \ldots \leftrightsquigarrow^+ v$. If $u \leftrightsquigarrow^+ v$, then from the algorithm of cyclical completion, there is a word w such

that $w \rightsquigarrow^* u$ and $w \rightsquigarrow^* v$. From Proposition 3.1, this implies $w \equiv_M u$ and $w \equiv_M v$ (modulo $\Re$), so $u \equiv_M v$ (modulo $\Re$). If $u \rightsquigarrow^+ u_2 \rightsquigarrow^+ u_3..u_k \rightsquigarrow^+ v$, then $u_i \equiv_M u_{i+1}$ (modulo $\Re$) from the first case, so $u \equiv_M v$ (modulo $\Re$). □

Given two complete and cyclically terminating rewriting systems $\Re$ and $\Re'$, we say that $\Re$ and $\Re'$ are *cyclically equivalent* if the following condition holds: $u \equiv_M v$ modulo $\Re'$ if and only if $u \equiv_M v$ modulo $\Re$. We show that the cyclical rewriting system $\Re^+$ obtained from the application of the algorithm of cyclical completion on $\Re$ is cyclically equivalent to $\Re$.

Lemma 6.3 *Let $\Re$ be a complete and cyclically terminating rewriting system, we assume that $\Re$ is finite. Let $\Re^+$ be the cyclical rewriting system obtained from the application of the algorithm of cyclical completion on $\Re$. Then $\Re^+$ and $\Re$ are cyclically equivalent, that is $u \equiv_M v$ modulo $\Re^+$ if and only if $u \equiv_M v$ modulo $\Re$.*

Proof It holds that $u \equiv_M v$ modulo $\Re$ if and only if there are words x, y in Σ^* such that $ux =_M xv$ and $yu =_M vy$. Since the (linear) rules in $\Re^+$ are the same as those in $\Re$, this holds if and only if $u \equiv_M v$ modulo $\Re^+$ also. □

We say that there is a *cyclical ambiguity* in w if $w \rightsquigarrow^* u$ and $w \rightsquigarrow^* v$, where u and v are not cyclic conjugates. If there exist cyclically conjugate words z and z' in Σ^* such that $u \rightsquigarrow^* z$ and $v \rightsquigarrow^* z'$, then we say that this cyclical ambiguity *resolves*. Clearly, a rewriting system is cyclically confluent if and only if all the cyclical ambiguities resolve. Now, we show that whenever the algorithm of cyclical completion does not fail, the rewriting system obtained $\Re^+$ is cyclically complete.

Proposition 6.4 *Let $\Re$ be a complete and cyclically terminating rewriting system, we assume that $\Re$ is finite. Let $\Re^+$ be the cyclical rewriting system obtained from the application of the algorithm of cyclical completion on $\Re$. Then $\Re^+$ is cyclically complete.*

Proof We need to show that $\Re^+$ is cyclically confluent. Clearly, by the application of the algorithm of cyclical completion on $\Re$ the cyclical overlaps and inclusions in $\Re$ are resolved. So, it remains to show that the addition of the new cyclical rules in $\Re^+$ does not create a cyclical ambiguity. If a cyclical ambiguity occurs, then there should be one of the following kind of rules in $\Re^+$:

- $u \rightsquigarrow^+ v$ and $l \rightarrow x$, where $l \simeq u$.
- $u \rightsquigarrow^+ v$ and $l \rightsquigarrow^+ x$, where $l \simeq u$.

The first case cannot occur, since u is cyclically irreducible modulo $\Re$ and the second case cannot occur, since in this case the algorithm of cyclical completion fails. □

7 Length-preserving rewriting systems

We say that a rewriting system $\Re$ is *length-preserving* if $\Re$ satisfies the condition that the left-hand sides of rules have the same length as their corresponding right-hand

sides. We show that if $\mathfrak{R}$ is a length-preserving rewriting system, then an infinite sequence of cyclical reductions occurs only if there is a repetition of some word in the sequence or if a word and its cyclic conjugate occur there. Using this fact, we define an equivalence relation on the words that permits us to obtain some partial results in the case that $\mathfrak{R}$ is not cyclically terminating.

Lemma 7.1 *Let $\mathfrak{R}$ be a complete rewriting system that is length-preserving. If there is an infinite sequence of cyclical reductions, then it contains (at two different positions) words that are cyclic conjugates.*

Proof From the assumption, applying $\mathfrak{R}$ on a word u does not change its length $\ell(u)$, so all the words appearing in such an infinite sequence have the same length. Since the number of words of length $\ell(u)$ is finite, an infinite sequence of cyclical reductions occurs only if it contains words that are cyclic conjugates at two different positions. $\square$

Note that using the same argument as in Lemma 7.1, we have that if $\mathfrak{R}$ is length-decreasing, that is all the left-hand sides of rules have length greater than their corresponding right-hand sides, then there is no infinite sequence of cyclical reductions, that is $\mathfrak{R}$ is cyclically terminating. In the following lemma, we show that if there is an infinite sequence of cyclical reductions that results from the occurrence of a word w and its cyclic conjugate $\tilde{w}$, then there are some relations of commutativity involving w and $\tilde{w}$. This is not clear if these relations of commutativity are a sufficient condition for the occurrence of an infinite sequence, nor if such a sufficient condition can be found.

Lemma 7.2 *Assume there is an infinite sequence $w \looparrowright^* \tilde{w}$, where $w \backsimeq \tilde{w}$. Then there are words x, y such that $yx\tilde{w} =_M \tilde{w}yx$ and $xyw =_M wxy$.*

Proof From Proposition 3.1, $w \equiv_M \tilde{w}$, that is there are words x, y in Σ^* such that $wx =_M x\tilde{w}$ and $yw =_M \tilde{w}y$. So, $wxy =_M x\tilde{w}y =_M xyw$ and $yx\tilde{w} =_M ywx =_M \tilde{w}yx$. $\square$

We now define the following equivalence relation $\sim$ on Σ^*. Let u, v be different words in Σ^*. We define $u \sim v$ if and only if $u \looparrowright^* v$ and $v \looparrowright^* u$, this is an equivalence relation. Clearly, if $\mathfrak{R}$ is cyclically terminating, then each equivalence class contains a single word, up to $\backsimeq$. Now, we show that there is a partial solution to the left and right conjugacy problem, using $\sim$ in the case that $\mathfrak{R}$ is not cyclically terminating. Note that given a word w such that Allseq(w) does not terminate, it may occur one of the following; either there is no cyclically irreducible form achieved in Allseq(w) (as in Example 2.2) or there is a unique cyclically irreducible form achieved in Allseq(w) (as in Example 4.2).

Proposition 7.3 *Let u and v be in Σ^*. If there exists a word z such that $u \sim z$ and $v \sim z$, then $u \equiv_M v$.*

Proof If there exists a word z such that $u \sim z$ and $v \sim z$, then from the definition of $\sim$ there are sequences $u \looparrowright^* z$ and $v \looparrowright^* z$. From Proposition 3.1, this implies $u \equiv_M z$ and $v \equiv_M z$, so $u \equiv_M v$. □

Note that the converse is not true as the following example illustrates it.

Example 7.1 Let $\Re = \{bab \rightarrow aba, ba^n ba \rightarrow aba^2 b^{n-1}, n \geq 2\}$. It holds that $a \equiv_M b$, since $a(aba) =_M (aba)b$ and $(aba)a =_M b(aba)$. Yet, there is no sequence of cyclical reductions such that $a \sim b$.

We can consider a rewriting system that is not length increasing (that is all the rules preserve or decrease the length) to be *cyclically terminating up to* $\sim$ and apply on it the algorithm of cyclical completion and obtain that it is *cyclically complete up to* $\sim$. This is due to the fact that also in this case infinite cyclical sequences would result from the occurrence of a word and its cyclic conjugate. If there exists a cyclically irreducible form then it is unique, but the existence of a cyclically irreducible form is not ensured. The complete and finite rewriting system $\Re$ from Example 2.5 illustrates this situation. It is not length increasing and not cyclically terminating, since there are infinite sequences of cyclical reductions (as an example $\Delta a \rightarrow b\Delta \circlearrowleft^1 \Delta b \rightarrow a\Delta$). The application of the algorithm of cyclical completion on $\Re$ gives $\Re^+ = \Re \cup \{\underline{ab} \looparrowright^+ \underline{ba}\}$ that is cyclically complete up to $\sim$. But, nevertheless there are words that have no cyclically irreducible form (Δa for example).

References

1. Book, R.V.: Confluent and other types of Thue systems. J. Assoc. Comput. Mach. **29**, 171–182 (1982)
2. Book, R.V., Otto, F.: String-Rewriting Systems. Springer, Berlin (1993)
3. Choffrut, C.: Conjugacy in free inverse semigroups. Int. J. Algebra Comput. **3**(2), 169–188 (1993)
4. Chouraqui, F.: Rewriting systems in alternating knot groups Int. J. Algebra Comput. **16**(4), 749–769 (2006)
5. Hermiller, S., Meier, J.: Artin groups, rewriting systems and three-manifolds. J. Pure Appl. Algebra **136**, 141–156 (1999)
6. Lentin, A., Schutzenberger, M.P.: A combinatorial problem in the theory of free monoids. Proc. Univ. North Carolina (1968), 128–144
7. McKnight, J.D., Storey, A.J.: Equidivisible semigroups. J. Algebra **12**, 24–48 (1969)
8. Narendran, P., Otto, F.: Complexity results on the conjugacy problem in monoids. Theor. Comput. Sci. **35**, 227–243 (1985)
9. Narendran, P., Otto, F.: The problems of cyclic equality and conjugacy for finite complete rewriting systems. Theor. Comput. Sci. **47**, 27–38 (1986)
10. Otto, F.: Conjugacy in monoids with a special Church-Rosser presentation is decidable. Semigroup Forum **29**, 223–240 (1984)
11. Pedersen, J., Yoder, M.: Term rewriting for the conjugacy problem and the braid groups. J. Symb. Comput. **18**(6), 563–572 (1994)

12. Silva, P.: Conjugacy and transposition for inverse monoid presentations Int. J. Algebra Comput. **6**(5), 607–622 (1996)
13. Sims, C.C.: Computing with Finitely Presented Groups. Wiley, New York (1996)
14. van Leeuwen, J. (ed.): Handbook of Theoretical Science. Formal Models and Semantics, vol. B. MIT Press, Cambridge (1990)
15. Zhang, L.: Conjugacy in special monoids. J. Algebra **143**(2), 487–497 (1991)