On Finite Semigroup Cross-Sections and Complete Rewriting Systems

António Malheiro
Centro de Álgebra da Universidade de Lisboa
Av. Prof. Gama Pinto 2, 1649-003 Lisboa, Portugal
and
Faculdade de Ciências e Tecnologia da UNL,
Quinta da Torre, 2829-516 Monte de Caparica, Portugal
E-mail: malheiro@cii.fc.ul.pt

Abstract

In this paper we obtain a [finite] complete rewriting system defining a semigroup/monoid S, from a given finite right cross-section of a subsemigroup/submonoid defined by a [finite] complete presentation. In the semigroup case the subsemigroup must have a right identity element which must also be part of the cross-section. In the monoid case the submonoid and the cross-section must include the identity of the semigroup. The result on semigroups allow us to show that if G is a group defined by a [finite] complete presentation then the completely simple semigroup M[G;1;J;P] is also defined by a [finite] complete rewriting system.

1. Introduction

One of the most important common topics of Computer Science and Mathematics is the word problem. This problem was initially formulated in the group theory by M. Dehn in 1912 [4]. However, it can be introduced in a natural way in the semigroup theory. A semigroup presentation \( \mathcal{P} \) is a pair \( \langle X \mid R \rangle \) where \( X \) is an alphabet and \( R \) is a rewriting system on \( X \), that is, a binary relation in the free semigroup on \( X \). Each semigroup presentation origins a semigroup \( S(\mathcal{P}) \) resultant of the quotient of the free semigroup \( X^+ \) by the Thue congruence \( \equiv^r \), generated by \( R \). This congruence is the symmetric, reflexive and transitive closure of the binary relation \( \rightarrow^r \) on \( X^+ \) given by: for any \( (r_{+1},r_{-1}) \in R \) and any words \( w_1 \) and \( w_2 \) on \( X^+ \), we have \( w_1r_{+1}w_2 \rightarrow^r w_1r_{-1}w_2 \). Now, the word problem can be formulated as follows: given words \( u \) and \( v \) in \( X^+ \), decide whether or not \( u \) and \( v \) represent the same element of \( S(\mathcal{P}) \), that is, decide if \( u \equiv^r \) \( v \). If there exists an algorithm which solves the word problem for any two words then the word problem is said to be solvable. The property of having solvable word problem is invariant for any finite presentation defining the same semigroup. Thus we can refer to the word problem of a given semigroup and not only to some of its finite presentations.

Finite and complete (that is, noetherian and confluent) rewriting systems are used to solve word problems among other algebraic decision problems (see [3, 8, 11] for examples). The word problem is solved using the ‘normal form algorithm’: given two words \( u \) and \( v \), we can calculate irreducible elements \( u_0 \) and \( v_0 \) such that \( u \equiv^r u_0 \) and \( v \equiv^r v_0 \), and we conclude that \( u \equiv^r v \) if and only if \( u_0 \) and \( v_0 \) are identical words. This application reveals the importance of such rewriting systems.

In Group Theory we say that a subgroup \( H \) has finite index in a group \( G \) if there are finitely many cosets \( Hg \), for any \( g \in G \). In that case we get \( G \) as a disjoint union of finitely many cosets \( H, Hg_1, \ldots, Hg_n \). The set \( \{1,g_1,\ldots,g_n\} \) is said to be a cross-section for \( H \) in \( G \). This means that each element in \( G \) is uniquely representable as the product of an element of \( H \) by an element of \( \{1,g_1,\ldots,g_n\} \). Groves and Smith [5] proved that if \( H \) is a subgroup of finite index in \( G \) and \( H \) has a [finite] complete rewriting system then \( G \) has a [finite] complete rewriting system. The main goal of this paper is to extend this result first for the monoid case and second to the semigroup case.

Let \( S \) be a semigroup and let \( M \) be a subsemigroup of \( S \). A [finite] subset \( T \) is said to be a [finite] (right) cross-section for \( M \) in \( S \) if any element of \( S \) can be uniquely factorized in the form \( mt \), with \( m \in M \) and \( t \in T \).

The first result can be stated without any other extra condition and as we will see the proof can be depicted from the group case.

Theorem 1.1 Let \( S \) be a monoid with identity element 1_s. Let \( M \) be a submonoid of \( S \) and let \( T \) be finite right cross-section for \( M \) in \( S \). Suppose that \( 1_s \in M \cap T \). If \( M \) is defined by a [finite] complete rewriting system, then \( S \) is also defined by a [finite] complete rewriting system.
Our second result requires an extra condition on the subsemigroup. We say the an element \( e \) of a semigroup \( M \) is a right identity element if \( me = m \), for any \( m \in M \).

**Theorem 1.2** Let \( S \) be a semigroup and let \( M \) be a subsemigroup of \( S \) having a right identity element \( e \). Suppose that there is a finite right cross-section for \( M \) in \( S \) including the element \( e \). If \( M \) is defined by a [finite] complete rewriting system, then \( S \) is also defined by a [finite] complete rewriting system.

This last result has a very important consequence in Semigroup Theory. A non-empty set \( A \) of a semigroup \( S \) is called a left ideal if \( SA \subseteq A \), a right ideal if \( AS \subseteq A \) and an ideal if it is both a left and a right ideal. Completely simple semigroups, among other characterizations (see [6]), are those semigroups with no proper ideals and with minimal left and right ideals.

In the 1920’s Suschkewitsch [12] has obtained a description of the completely simple semigroups in the following terms: let \( G \) be a group, let \( I \) and \( J \) be non-empty sets and let \( P = (p_{ji}) \) be a \( J \times I \) matrix with entries in \( G \); the set \( I \times G \times J \) with multiplication

\[
(i_1,s_1,j_1)(i_2,s_2,j_2) = (i_1,s_1p_{j_1i_2},j_2),
\]
is a completely simple semigroup; conversely, every completely simple semigroup is isomorphic to a semigroup constructed in this way. The semigroup constructed as above is denoted by \( M[G; I, J, P] \) and it is called the \( I \times J \) Rees matrix semigroup over the group \( G \) with the sandwich matrix \( P \).

This description will allow us to use the above theorem and conclude the following about completely simple semigroups:

**Theorem 1.3** Let \( G \) be a group, let \( I \) and \( J \) be non-empty finite sets and let \( P = (p_{ji}) \) be a \( J \times I \) matrix with entries in \( G \). If the group \( G \) is defined by a [finite] complete rewriting system then the completely simple semigroup \( M[G; I, J, P] \) is also defined by a [finite] complete rewriting system.

To understand the finiteness condition on the sets \( I \) and \( J \) on the above result it is essential to have in mind the result [2] by H. Ayik and N. Ruškuc, where the authors consider finite presentability of Rees matrix semigroups. They have conclude that the Rees matrix semigroup \( M[G; I, J, P] \) is finitely presented (i.e., defined by a finite rewriting system over a finite alphabet) if and only if the group \( G \) is finitely presented and the sets \( I \) and \( J \) are finite.

After some preliminaries on Section 2, we turn, in Section 3, to the proof of Theorem 1.2. It follows a section dedicated to the proof of Theorem 1.1 and we finish with Section 4 where we prove Theorem 1.3.

## 2. Preliminaries

Let \( X \) be an alphabet. We denote by \( X^* \) the free monoid on \( X \) and by \( X^+ \), the free semigroup on \( X \). For an element of \( X^* \), a word \( w \), we denote the length of \( w \) by |\( w \)|.

A rewriting system is a pair \((X, R)\), where \( X \) is an alphabet and \( R \) is a binary relation in \( X^* \). The elements of \( R \) are referred to as rewriting rules. Usually, a rewriting rule \( r \in R \) is written in the form \( r = (r_{+1}, r_{-1}) \) or, simply, \( r_{+1} \rightarrow r_{-1} \). In the following the rewriting system will be simply denoted by \( R \). We say that a rewriting system \( R \) is finite if both \( R \) and \( X \) are finite.

In \( X^* \) we define a binary relation, \( \rightarrow_R \), denoted as single-step reduction, in the following way:

\[
u \rightarrow_R v \iff u = w_1 r_{+1} w_2 \text{ and } v = w_1 r_{-1} w_2
\]

for some \((r_{+1}, r_{-1}) \in R \) and \( w_1, w_2 \in X^* \). The transitive and reflexive closure of \( \rightarrow_R \) is denoted by \( \rightarrow^* \). By \( \rightarrow^R \) we denote the transitive closure of \( \rightarrow_R \). A word \( u \in X^* \) is said to be \( R \)-irreducible, if there is a word \( v \in X^* \) such that \( u \rightarrow^R v \). If a word is not \( R \)-reducible, it is called \( R \)-irreducible or simply irreducible. By \( \text{Irr}(R) \) we denote the set of all \( R \)-irreducible words.

By \( \equiv^R_h \) we denote the equivalence relation induced by \( \rightarrow_h \) which is a congruence on the free monoid \( X^* \). The quotient of the free monoid \( X^* \) by what is called the Thue congruence \( \equiv^R_h \) generated by \( R \) gives the monoid defined by \( R \) and it is denoted by \( M(X; R) \). The set \( X \) is called the generating set and \( R \) the set of defining relations. More generally, a monoid is said to be defined by the rewriting system \( R \) if \( M \cong M(X; R) \). Thus, the elements of \( M \) are identified with congruence classes of words from \( X^* \). We will sometimes identify words and elements they represent.

We say that a rewriting system \( R \) on \( X \) is noetherian if the relation \( \rightarrow_R \) is well-founded, in other words, if there is no infinite descending chains

\[
w_1 \rightarrow_R w_2 \rightarrow_R w_3 \rightarrow_R \cdots \rightarrow_R w_n \rightarrow_R \cdots
\]

We say that \( R \) is confluent if whenever we have \( u \rightarrow^R_h v \) and \( u \rightarrow^R_h v' \) there is a word \( w \in X^* \) such that \( v \rightarrow^R_h w \) and \( v' \rightarrow^R_h w \). If \( R \) is simultaneously noetherian and confluent we say that \( R \) is complete.

It is easy to verify that, if \( R \) is a noetherian rewriting system, each congruence class of \( M(X; R) \) contains at least one irreducible element. Assuming \( R \) noetherian, then \( R \) is a complete rewriting system if and only if each congruence class of \( M(X; R) \) contains exactly one irreducible element [3]. Hence, a complete rewriting system fixes a unique normal form for each of its congruence classes.

A sufficient condition for a rewriting system \( R \) be noetherian is given in the following lemma.
Lemma 2.1 Let $R$ be a rewriting system on an alphabet $X$ and let $>$ be a binary relation irreflexive, transitive and well-founded in $X^*$. 

1. If $>$ satisfies $u \rightarrow_k v$ implies $u > v$, then $R$ is noetherian.

2. If $>$ satisfies $(u, v) \in R$ implies $u > v$ and $u > v$ implies that $w_1uv_2 > w_1vw_2$, for all $w_1, w_2 \in X^*$, then $R$ is noetherian.

Let $S$ be a monoid. Given a surjective morphism $\phi : X^* \rightarrow S$ and a noetherian rewriting system $R$ on $X$, the following proposition gives us sufficient conditions to guarantee that there exist a complete rewriting system for $S$.

Proposition 2.2 Let $S$ be a monoid and $R$ a noetherian rewriting system on $X$. Let $\phi : X^* \rightarrow S$ be a surjective morphism such that

1. $\phi(r_{+1}) = \phi(r_{-1})$, for each relation $(r_{+1}, r_{-1}) \in R$.
2. the restriction of $\phi$ to $\text{Irr}(R)$ is one-to-one.

Then $R$ is a complete rewriting system that defines $S$.

In the above concepts is clear that if we replace monoid by semigroup and $X^*$ by $X^+$ we obtain similar definitions and we still with valid results.

It is important to notice that for a noetherian rewriting system $R$ on a set $X$ there only exists a finite number of descending chains starting at a word $u$ of $X^*$. Thus there exists a maximum on the length of any word appearing on all descending chains starting at a word $u$ of $X^*$. That maximum is called the stretch of $u$ and it is denoted by $\text{str}(u)$. Observe that if $\text{str}(u) > \text{str}(v)$ then $\text{str}(u_1uw_2) > \text{str}(w_1vw_2)$, for any words $w_1, w_2 \in X^*$; that is, the stretch is compatible with the concatenation product.

Further information on rewriting systems can be found in [3].

3. Cross-sections - the semigroup case

This section is dedicated to the proof of Theorem 1.2. Let $S$ be a semigroup and let $M$ be a subsemigroup of $S$ having a right identity $e$. Suppose that there exists a finite right cross-section $T$ for $M$ in $S$. Also, suppose that $e$ belongs to $T$.

We observe that any element $t$ of the cross-section is an element in $S$ and hence it is factorized in the form $mt$, for some $m \in M$ and $t' \in T$. Thus we have an element $et = emt'$ in $S$. It follows from the uniqueness of the decomposition of the elements in $S$ that $t = t'$. Concluding, any element $t$ of the cross-section is equal to $mt$, for some $m_t \in M$.

Let $R$ be a [finite] complete rewriting system on an alphabet $X$. Denote by $e$ the word in $X^+$ representing the right identity of $M$.

Let $Y$ be an alphabet disjoint from $X$ in one-to-one correspondence with $T$. Denote by $u$ the letter in $Y$ representing the right identity of $M$ which as we have supposed it also belongs to $T$. So we have $u = e$, that is, $u$ is equal to $e$ in $S$.

If we define a correspondence from $X \cup Y$ to $S$ by associating any element in $X$ to the corresponding representant in $M$ (and thus in $S$) and to any element of $Y$ the correspondent element of $T$, and we extend it to $(X \cup Y)^+$ we will clearly obtain a surjective morphism. Along this section we will identify the elements of $(X \cup Y)^+$ with the corresponding elements of $S$.

It might be now clear to the reader that we will use Proposition 2.2 to prove that $S$ is defined by a [finite] complete rewriting system.

Let us consider the following sets of rewriting rules on the alphabet $X \cup Y$:

$R_1 = \{ wz \rightarrow xv : w, z, v \in Y, x \in \text{Irr}(R), wz =_s xv \}$

$R_2 = \{ wx \rightarrow yv : w, v \in Y, x \in X, y \in \text{Irr}(R), wx =_s yv \}$

$R_3 = \{ yv \rightarrow w : w \in Y, y \in \text{Irr}(R), yv =_s w \}$

$R_4 = \{ u \rightarrow e \}$

Now, denote by $R'$ the set $R \cup R_1 \cup R_2 \cup R_3 \cup R_4$. Notice that if $T$ is finite and $(X \mid R)$ is finite then $R'$ is also finite.

We have to see if these rules are valid in $S$. We observe that each element of $S$ can factorized in the form $mt$, with $m \in M$ and $t \in T$. Also, each element $t \in T$ is of the form $m_t$, for some $m_t \in M$. Together with these observations we see that the rewriting rules of $R'$ are obtained when they are equalities in $S$, so we may conclude that they are valid in $S$.

We claim that the set of irreducible elements of the rewriting system $R'$ on the alphabet $X \cup Y$ is $(\text{Irr}(R) \setminus \{ y \in Q \}) \cup Y \setminus \{ u \} \cup \text{Irr}(R)$, where $Q$ is the set $\{ y \in \text{Irr}(R) : yw =_s w, w \in Y \}$. We begin by observing that if we start with a word in $(X \cup Y)^+$ with at least one letter from $Y$ we can: first apply rewriting rules from $R_2$ to obtain a word in the form $zv$, with $z \in X^+$ and $v \in Y^+$; then we can apply rewriting rules from $R_1$ to $v$ to obtain a word of the form $z'v'$, with $z' \in X^+$ and $v' \in Y$; now, if $v' = u$ we apply the rewriting rule from $R_3$ and we end up with a word in $X^+$; in any case to the remaining word of $X^+$ we apply the rewriting rules from $R$ to get an element in $\text{Irr}(R)$. If we get a factorization of the form $yw$, with $y \in Q$ and $w \in Y \setminus \{ u \}$, we apply a rewriting rule from $R_3$ to obtain a word in $Y \setminus \{ u \}$. Finally, if we have a word in $X^+$ we apply rewriting rules from $R$ to get a word in $\text{Irr}(R)$. The final set of irreducible elements will be the set claimed above.

As already mentioned each element of $S$ is uniquely representable as the product of an element of $M$ and an ele-
element of $T$. Clearly the set $M(T \{e\})$ is in one-to-one correspondence with $(\operatorname{Irr}(R) \{y \in Q\}) \cup Y \{u\}$ and $Me = M$ is in one-to-one correspondence with $\operatorname{Irr}(R)$. Thus we conclude that $S$ is one-to-one correspondence with our set of irreducible elements of $R'$.

According to Proposition 2.2 it remains to show that the rewriting system is noetherian. In order to follow that propose we will introduce a binary relation $>_S$ on the set $(X \cup Y)^+$ that it is irreducible, transitive and well-founded. Moreover this relation is also compatible with the concatenation product. Hence we will use Lemma 2.1(2) to prove that $R$ is noetherian.

A word $z$ in $(X \cup Y)^+$ has the form

$$x_nu_nx_{n-1} \cdots x_1u_1x_0,$$

with $n \in \mathbb{N}_0$, $u_i \in Y$, and $x_j \in X^*$. Let us define maps

$$\psi_0(z) = |u_n \cdots u_1| = n,$$
$$\psi_{i+1}(z) = \mathfrak{R}(x_{i-1}),$$
$$\psi(z) = x_{i-1},$$

for $i \in \{1, \ldots, n + 1\}$. We define $>_S$ by: given $z_1, z_2 \in (X \cup Y)^+$, we have $z_1 >_S z_2$ if it exists $k \in \mathbb{N}_0$ such that $\psi_i(z_1) = \psi_i(z_2)$, for $i < k$, and $\psi_k(z_1) > \psi_k(z_2)$ (if $k$ odd or 0) and $\psi_k(z_1) > \psi_k(z_2)$ (if $k$ is even).

Finally, we claim that $u > v$ for each $(u, v) \in R'$. Let us see case by case:

- if $(u, v) \in R$ then $\psi_0(u) = \psi_0(v)$, $\psi_1(u) \geq \psi_1(v)$ and $\psi_2(u) \rightarrow_S \psi_2(v)$;
- if $(u, v) \in R_1$ then $\psi_0(u) > \psi_0(v)$;
- if $(u, v) \in R_2$ then $\psi_0(u) = \psi_0(v)$ and $\psi_1(u) > \psi_1(v)$;
- if $(u, v) \in R_3$ then $\psi_i(u) = \psi_i(v)$, for $i = 0, 1, 2$, and $\psi_3(u) > \psi_3(v)$ and $\psi_3(u) > \psi_3(v)$;
- if $(u, v) \in R_4$ then $\psi_0(u) > \psi_0(v)$.

Thus $R$ is noetherian. It follows from Proposition 2.2 that $R'$ is a [finite] complete rewriting system on $(X \cup Y)^+$ that defines the semigroup $S$.

4. Cross-sections - the monoid case

In this section we will prove Theorem 1.1. So let $S$ be a monoid and let $M$ be a submonoid of $S$ with $1_S \in M$. Also, suppose that there is a finite right cross-section $T$ for $M$ in $S$ with $1_S \in T$.

The proof of Theorem 1.1 follows the same idea of the previous case, the semigroup case. In fact we can say that it is a simplified version of it. We will only sketch the proof pointing out the differences.

In this case we are working on the free monoids over $X$ and over $X \cup Y$ and therefore including the empty word. Thus we don’t need to distinguish a word representing the identity of $M$ which is also the identity of $S$. Also the set $Y$ will be in one-to-one correspondence with $T' \{1\}$.

The factorization of the elements in $T$ is trivial in this case, since each $t \in T$ is uniquely decomposed in the form $1st$, with $1_S \in M$ and $t \in T$. Thus we will not have the set $R_3$ in our final rewriting system.

We consider the sets $R_1$ and $R_2$ of rewriting rules

$$\{wz \rightarrow xv : w, z \in Y, v \in Y \cup \{1\}, x \in \operatorname{Irr}(R), wz =_S xv\}$$
$$\{wx \rightarrow yv : w \in Y, v \in Y \cup \{1\}, x \in X, y \in \operatorname{Irr}(R), wx =_S yv\},$$

respectively, on the alphabet $X \cup Y$. Let $R'$ be the set $R_1 \cup R_2$. If $T$ is finite and $(X \mid R)$ is finite then $R'$ is also finite.

In this case it is clear that the set of irreducible elements is $\operatorname{Irr}(R) \cup \operatorname{Irr}(R)Y$, that is in one-to-one correspondence with $S$.

Keeping the same relation ordering we also conclude that $u > v$ whenever $(u, v) \in R'$. The slightly changes on the sets $R_1$ and $R_2$ (notice that now $v$ may be the empty word) can only lead us to the conclusion that $\psi_0(u) > \psi_0(v)$. Hence we can also say that $R'$ is noetherian. Therefore, by Proposition 2.2, the rewriting system $R'$ is [finite] complete and it defines the monoid $S$.

5. Completely simple semigroups

The isomorphism mentioned in the Introduction between a completely simple semigroup and a $I \times J$ Rees matrix semigroup over the group $G$ with the sandwich matrix $P$ can be, in a certain sense, normalized. It is possible to find a sandwich matrix $P$, which it will be called normal, having more appropriate entries.

Let $G$ be a group, let $I$ and $J$ be non-empty finite sets and let $P = (p_{ij})$ be a $I \times J$ matrix with entries in $G$. Without lost of generality we can suppose that both sets $I$ and $J$ have an element named 1 and that the first column has elements $p_{1i}$’s and the first row $p_{1j}$’s. Let $e$ denote the identity element of the group $G$. The sandwich matrix $P$ is called normal if every entry in the first row and in the first column of $P$ is equal to $e$.

The normalization theorem says that if $S$ is a completely simple semigroup then $S$ is isomorphic to a Rees matrix semigroup $M(G; I; J; P)$ in which the matrix $P$ is normal. The isomorphism from $S = M(G; I; J; Q)$ to $M(G; I; J; P)$, with $Q = [q_{ij}]$, not necessarily normal, is obtained from the correspondence $(i, a, j) \rightarrow (i, q_{ij}^{-1}q_{ia}aq_{ij}, j)$, and where $P = p_{ij} = q_{ij}^{-1}q_{ij}q_{ij}$ is normal (see [6] for more details). From now on we will assume that the sandwich matrix $P$ is normal.
The subsemigroup \( \{1\} \times G \times \{1\} \) has an identity element \((1, e, 1)\). The set \( \{1\} \times \{e\} \times J \) is a finite right cross-section for \( \{1\} \times G \times \{1\} \) in \( \{1\} \times G \times J \) since each word \((1, a, j)\) is uniquely decomposed as \((1, a, 1)(1, e, j)\), with \((1, a, 1) \in \{1\} \times G \times \{1\}\) and \((1, e, j) \in \{1\} \times \{e\} \times J\).

Suppose that \( G \) is defined by a [finite] complete rewriting system. By Theorem 1.2 we conclude that \( \{1\} \times G \times J \) is defined by a [finite] complete rewriting system.

Now, \( \{1\} \times G \times J \) has a left identity \((1, e, 1)\). Also, the set \( I \times \{e\} \times \{1\} \) is a finite left cross-section for \( \{1\} \times G \times J \) in \( M[G; I, J; P] \). Thus, by applying the dual of Theorem 1.2 for left cross-sections we get the intended result, that is, \( M[G; I, J; P] \) is defined by a [finite] complete rewriting system.

6. Conclusion

Completely simple semigroups are an important class of semigroups. The problem of relating the properties of the group \( G \) with the properties of the semigroup \( M[G; I, J; P] \) was studied in several papers (see for example [1, 2, 7, 9, 10]).

Concerning complete rewriting systems we have proved that if \( G \) is defined by a [finite] complete rewriting system and both \( I \) and \( J \) are finite then \( M[G; I, J; P] \) is also defined by a [finite] complete rewriting system. We end with the following natural question:

**Open Problem:** If a finitely presented completely simple semigroup \( S = M[G; I, J; P] \) is defined by a complete rewriting system is then \( G \) also defined by a complete rewriting system.

Acknowledgements

This work was developed within the project POCTI-ISFL-1-143 of CAUL, financed by FCT and FEDER. It is also part of the project "Semigroups and Languages - PTDC/MAT/69514/2006", financed by FCT.

References