Theoretical Computer Science 409 (2008) 537–548

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Rational subsets of partially reversible monoids

Pedro V. Silva *

Centro de Matemática, Faculdade de Ciências, Universidade do Porto, R. Campo Alegre 687, 4169-007 Porto, Portugal

ARTICLE INFO

Article history:
Received 29 December 2005
Received in revised form 31 May 2008
Accepted 12 September 2008
Communicated by M. Ito

Keywords:
Rational
Recognizable
Rewriting systems
Reversibility

ABSTRACT

A class of monoids that can model partial reversibility allowing simultaneously instances of two-sided reversibility, one-sided reversibility and no reversibility is considered. Some of the basic decidability problems involving their rational subsets, syntactic congruences and characterization of recognizability, are solved using purely automata-theoretic techniques, giving further insight into the structure of recognizable languages.

1. Introduction

Given an alphabet X, we denote by X^{-1} a set of formal inverses of X and we write $X^{\pm 1} = X \cup X^{-1}$.

We call *partially reversible* monoid (PR-monoid) a monoid defined by a finite monoid presentation of the form $\mathrm{Mon}\langle X \mid R\rangle$, where

$$X = X_0 \cup X_1^{\pm 1} \cup X_2^{\pm 1}$$

is a disjoint union and

$$R = \{xx^{-1} = 1 \mid x \in X_1 \cup X_2^{\pm 1}\}.$$

We recall that the *bicyclic* monoid is defined by a finite monoid presentation of the form

$$\mathrm{Mon}\langle x^{\pm 1} \mid xx^{-1} = 1\rangle.$$

The above PR-monoid can then be described as the free product of the free monoid X_0^*, $|X_1|$ copies of the bicyclic monoid and the free group on X_2.

PR-monoids can be defined through the rewriting system

$$\{xx^{-1} \to 1,\ x \in X_1 \cup X_2^{\pm 1}\}$$

on X. This is a particular case of the wider class of finite special (and therefore monadic) confluent rewriting systems. Algorithmic properties of special rewriting systems were considered in Adyan's fundamental monograph [1]. We shall also consider further generalizations, namely rational length-reducing left basic rewriting systems.

After Section 2, where notation, terminology and preliminary results are introduced, we summarize in Section 3 some basic results involving rational subsets of monoids defined by rational length-reducing left basic confluent rewriting

* Tel.: +351 220100751; fax: +351 220100751.
E-mail address: pvsilva@fc.up.pt.
URL: http://www.fc.up.pt/cmup.

0304-3975/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2008.09.031

systems. The most general versions of these results are due to Sénizergues [9]. As a consequence, the property of being recognizable is proved to be decidable, but the complexity is at least double exponential.

In Section 4 we introduce PR-monoids and show that the syntactic monoid of an arbitrary rational subset A has always a solvable word problem. The algorithm we present is fully automata-theoretic and has polynomial complexity with respect to the minimal automaton of the reduced language $\overline{A}$.

This result is applied in Section 5, where we characterize recognizable subsets among rational subsets of PR-monoids. The corresponding algorithm is much more efficient than the one in Section 3 for the general case of rational length-reducing left basic confluent rewriting systems, its complexity being polynomial on similar terms to those in Section 4. The results in Sections 4 and 5 generalize those obtained in [10] and [13] for the case of rational subsets of the free group. Similar problems are considered for other classes of groups in [14].

2. Preliminaries

The reader is referred to [3] and [6] (respectively [4]) for basic facts concerning languages and automata (respectively rewriting systems).

Whenever possible, brackets will be omitted in the representation of singular sets.

Let M be a monoid. Given $A, B \subseteq M$, we write $AB = \{ab \mid a \in A, b \in B\}$ and we denote by A^* the submonoid of M generated by A. We denote by $\mathrm{Rat}\, M$ the smallest family $\mathcal{F}$ of subsets of M such that:

- every finite subset of M is in $\mathcal{F}$;
- if $A, B \in \mathcal{F}$, then $A \cup B, AB, A^* \in \mathcal{F}$.

The elements of $\mathrm{Rat}\, M$ are called *rational* subsets of M. Alternatively, $A \subseteq M$ is said to be rational if A can be obtained from finite subsets of M using finitely many times the operators union, product and star.

Given $A \subseteq M$, we define a relation $\sim_A$ on M by $u \sim_A v$ if

$$puq \in A \Leftrightarrow pvq \in A$$

holds for all $p, q \in M$. The relation $\sim_A$ is a congruence on M, the *syntactic* congruence of A. We say that A is a *recognizable* subset of M if the congruence $\sim_A$ has finite index (i.e., the monoid $M/\sim_A$ is finite). We denote the set of all recognizable subsets of M by $\mathrm{Rec}\, M$. Alternatively, $A \subseteq M$ is recognizable if there exists some homomorphism $\varphi : M \to N$ into a finite monoid N such that $A\varphi\varphi^{-1} \subseteq A$. In this case, we have necessarily

$$\{(u, v) \in M \times M \mid u\varphi = v\varphi\} \subseteq \sim_A .$$

It is well known that $\mathrm{Rec}\, M$ constitutes a Boolean algebra [3, Proposition III.1.1].

The following elementary result will prove useful in forthcoming sections:

Lemma 2.1. *Let $\varphi : M \to N$ be a surjective monoid homomorphism and let $A \subseteq N$. Write $\sigma = \sim_{A\varphi^{-1}}$ and $\tau = \sim_A$. Then*

$$M/\sigma \to N/\tau : x\sigma \mapsto (x\varphi)\tau$$

is a monoid isomorphism.

A proof can be found in [13]. In the particular case of a free monoid X^* over a finite set X, Kleene's Theorem states that $\mathrm{Rat}\, X^* = \mathrm{Rec}\, X^*$, and the class can be characterized as the class of languages recognized by finite automata.

We denote a finite X-automaton as a quadruple $\mathcal{A} = (Q, i, T, E)$ where $i \in Q$ is the initial state, $T \subseteq Q$ are the terminal states and

$$E \subseteq Q \times (X \cup 1) \times Q.$$

The language recognized by $\mathcal{A}$ is denoted by $L(\mathcal{A})$ and we write

$$L_{in}(\mathcal{A}) = L(Q, i, Q, E).$$

If the automaton $\mathcal{A}$ is deterministic then, given $q \in Q$ and $w \in X^*$, we denote by qw the unique state of $\mathcal{A}$ such that there is a path of the form $q \xrightarrow{w} qw$ in $\mathcal{A}$, if such a path exists. Otherwise, we write $qw = \emptyset$. The *accessible* part of $\mathcal{A}$ is defined by

$$\mathrm{acc}(\mathcal{A}) = (Q', i, T \cap Q', E \cap (Q' \times (X \cup 1) \times Q')),$$

where $Q' = \{q \in Q \mid L(Q, i, q, E) \neq \emptyset\}$. We say that $\mathcal{A}$ is *accessible* if $\mathrm{acc}(\mathcal{A}) = \mathcal{A}$. Given $L \in \mathrm{Rat}\, X^*$ nonempty, we denote by min_L the *minimal* automaton of L.

Given X-automata $\mathcal{A} = (Q, i, T, E)$ and $\mathcal{A}' = (Q', i', T', E')$, we define the *direct product*

$$\mathcal{A} \times \mathcal{A}' = (Q \times Q', (i, i'), T \times T', E''),$$

where

$$E'' = \{((p, p'), x, (q, q')) \mid (p, x, q) \in E,\ (p', x, q') \in E'\}.$$

Given $L \subseteq X^*$, we denote by $\mathrm{Pref}(L)$ the set of all prefixes of words in L. A language $L \subseteq X^*$ is said to be *prefix-closed* if $\mathrm{Pref}(L) = L$.

Lemma 2.2. *Let $L, L' \in \mathrm{Rat}\, X^*$ be such that $L \subseteq L'$ and L' is prefix-closed. Then there exists a finite deterministic accessible X-automaton $\mathcal{A}$ such that $L(\mathcal{A}) = L$ and $L_{in}(\mathcal{A}) = L'$.*

Proof. We may assume that $L' \neq \emptyset$. Let $\mathcal{A}_1 = (Q_1, i_1, T_1, E_1)$ be a finite deterministic complete X-automaton recognizing L (it may be obtained through the subset construction) and let $\mathcal{A}_2 = (Q_2, i_2, T_2, E_2) = \min_{L'}$. Let $\mathcal{A} = \mathrm{acc}(\mathcal{A}_1 \times \mathcal{A}_2)$. Then

$$\begin{aligned} L(\mathcal{A}) &= L(\mathrm{acc}(\mathcal{A}_1 \times \mathcal{A}_2)) = L(\mathcal{A}_1 \times \mathcal{A}_2) \\ &= L(\mathcal{A}_1) \cap L(\mathcal{A}_2) = L \cap L' = L. \end{aligned}$$

On the other hand, writing $\mathcal{A}_1 \times \mathcal{A}_2 = (Q_1 \times Q_2, (i_1, i_2), T_1 \times T_2, E)$, we have

$$\begin{aligned} L_{in}(\mathcal{A}) &= L_{in}(\mathrm{acc}(\mathcal{A}_1 \times \mathcal{A}_2)) = L_{in}(\mathcal{A}_1 \times \mathcal{A}_2) \\ &= L(Q_1 \times Q_2, (i_1, i_2), Q_1 \times Q_2, E) = L((Q_1, i_1, Q_1, E_1) \times (Q_2, i_2, Q_2, E_2)) \\ &= L_{in}(\mathcal{A}_1) \cap L_{in}(\mathcal{A}_2) = X^* \cap \mathrm{Pref}(L') \\ &= X^* \cap L' = L' \end{aligned}$$

as required. □

Let X be a finite alphabet. A *rewriting system* on X is a subset $\mathcal{R}$ of $X^+ \times X^*$. We denote by $\mathcal{R}_1$ (respectively $\mathcal{R}_2$) the projection of $\mathcal{R}$ into the first (respectively second) component. Given $u, v \in X^*$, we write $u \longrightarrow v$ if

$$u = arb, \quad v = asb$$

for some $a, b \in X^*$ and $(r, s) \in \mathcal{R}$. We write $u \xrightarrow{*} v$ if

$$u = w_0 \longrightarrow w_1 \longrightarrow \cdots \longrightarrow w_n = v$$

for some $w_0, \ldots, w_n \in X^*$ ($n \geq 0$). The rewriting system $\mathcal{R}$ is said to be

- *finite* if $\mathcal{R}$ is finite;
- *rational* if $\mathcal{R} = \cup_{i=1}^{n} L_i \times \{u_i\}$ with $L_i \in \mathrm{Rat}\, X^*$ and $u_i \in X^*$ for $i = 1, \ldots, n$;
- *length-reducing* if $(r, s) \in \mathcal{R} \Rightarrow |r| > |s|$;
- *monadic* if it is length-reducing and $\mathcal{R} \subseteq X^+ \times (X \cup 1)$;
- *special* if $\mathcal{R} \subseteq X^+ \times 1$;
- *left basic* if $\mathcal{R}_2 \cap X^+ \mathcal{R}_1 = \emptyset$ and

  $$\forall u \in \mathcal{R}_2,\ X^* u \cap X^* \mathcal{R}_1 Y_{|u|} = \emptyset,$$

  where $Y_{|u|} = \{v \in X^+ : |v| < |u|\}$;
- *confluent* if, for all $u, v, w \in X^*$ such that

  $$u \xrightarrow{*} v, \quad u \xrightarrow{*} w,$$

  there exists some $z \in X^*$ such that

  $$v \xrightarrow{*} z, \quad w \xrightarrow{*} z;$$

- *locally confluent* if, for all $u, v, w \in X^*$ such that

  $$u \longrightarrow v, \quad u \longrightarrow w, \quad v \neq w$$

  there exists some $z \in X^*$ such that

  $$v \xrightarrow{*} z, \quad w \xrightarrow{*} z.$$

Let $\mathcal{R}$ be a length-reducing confluent rewriting system on X. We say that $u \in X^*$ is *irreducible* if no word $v \in X^*$ satisfies $u \to v$. Since $\mathcal{R}$ is length-reducing, for every $u \in X^*$ there is at least one irreducible word v satisfying $u \xrightarrow{*} v$. Since $\mathcal{R}$ is confluent, this word is unique and we denote it by $\overline{u}$. In particular, $\overline{X^*}$ denotes the set of all irreducible words on X.

The monoid defined by a rewriting system $\mathcal{R}$ on X is the quotient $M = X^*/\mathcal{R}^\sharp$, where $\mathcal{R}^\sharp$ denotes the congruence on X^* generated by the relation $\mathcal{R}$. Note that $(u, v) \in \mathcal{R}^\sharp$ if and only if there exists a finite sequence of words $u = w_0$, $w_1, \ldots, w_{n-1}, w_n = v$ ($n \geq 0$) such that

$$\forall i \in \{1, \ldots, n\}\ \exists a_i, b_i \in X^*,\ \exists (r_i, s_i) \in R :\ \{w_{i-1}, w_i\} = \{a_i r_i b_i, a_i s_i b_i\}.$$

Let $\pi : X^* \to M$ denote the canonical homomorphism. If $\mathcal{R}$ is length-reducing and confluent, then $u\pi = \overline{u}\pi$ for every $u \in X^*$ and the equivalence

$$u\pi = v\pi \Leftrightarrow \overline{u} = \overline{v}$$

holds for all $u, v \in X^*$.

3. General results

The well-known Benois Theorem on rational subsets of the free group [2] can be generalized to rational length-reducing left basic confluent rewriting systems by the results of Sénizergues, valid for the more general notion of *controlled* rewriting system, where we associate to each $(r, s) \in \mathcal{R} \subseteq X^+ \times X^*$ a language $K(r, s) \subseteq X^*$ and we write $u \longrightarrow v$ if $u = arb$ and $v = asb$ for some $(r, s) \in \mathcal{R}$, $a \in K(r, s)$ and $b \in X^*$. Clearly, if $K(r, s) = X^*$ for every $(r, s) \in \mathcal{R}$, we have the usual concept of rewriting system. By [9, Theorem 3.8], any rational length-reducing left basic confluent controlled rewriting system can be transformed into some *finite* length-reducing left basic confluent controlled rewriting system generating the same congruence and the same set of irreducible words. Now [9, Theorem 3.8] yields:

Theorem 3.1. *[9] Let $\mathcal{R}$ be a rational length-reducing left basic confluent rewriting system on X and let $L \in \operatorname{Rat} X^*$. Then $\overline{L} \in \operatorname{Rat} X^*$.*

In particular, the theorem holds for finite monadic confluent rewriting systems.

Note that, given a monoid M and a homomorphism $\varphi : X^* \to M$, the rational subsets of M are precisely the subsets of the form $L\varphi$ with $L \in \operatorname{Rat} X^*$ [3, Prop. III.2.2]. This characterization will be used throughout the paper without further comment.

Now we can easily deduce from Theorem 3.1 the following characterization of rational subsets, well known in the particular case of the free group as *Benois Theorem* [2]:

Corollary 3.2. *Let $\mathcal{R}$ be a rational length-reducing left basic confluent rewriting system on X and let $L \subseteq X^*$. Let $\pi : X^* \to M = X^*/\mathcal{R}^\sharp$ be the canonical homomorphism. Then*

$$L\pi \in \operatorname{Rat} M \Leftrightarrow \overline{L} \in \operatorname{Rat} X^*.$$

Proof. Assume that $L\pi \in \operatorname{Rat} M$. Then we have $L\pi = L'\pi$ for some $L' \in \operatorname{Rat} X^*$. Therefore $\overline{L}\pi = L\pi = L'\pi = \overline{L'}\pi$. Now Theorem 3.1 yields $\overline{L} = \overline{L'} \in \operatorname{Rat} X^*$.

Conversely, assume that $\overline{L} \in \operatorname{Rat} X^*$. Then

$$L\pi = \overline{L}\pi \in \operatorname{Rat} M. \quad \square$$

Another straightforward consequence is stated in the next corollary, which generalizes a well-known property of $\operatorname{Rat} X^*$.

Corollary 3.3. *Let M be the monoid defined by a rational length-reducing left basic confluent rewriting system $\mathcal{R}$ on a finite alphabet X. Then $\operatorname{Rat} M$ is closed under the Boolean operations.*

Proof. Since $\operatorname{Rat} M$ is closed under union by definition, it is enough to show that $\operatorname{Rat} M$ is closed under complementation. Let $\pi : X^* \to M = X^*/\mathcal{R}^\sharp$ be the canonical homomorphism and let $A \in \operatorname{Rat} M$. Then $A = L\pi$ for some $L \in \operatorname{Rat} X^*$. By Theorem 3.1, we have $\overline{L} \in \operatorname{Rat} X^*$ and so $\overline{X^*} \setminus \overline{L} \in \operatorname{Rat} X^*$. We show that

$$M \setminus A = (\overline{X^*} \setminus \overline{L})\pi. \tag{1}$$

Let $u\pi \in M \setminus A$, with $u \in X^*$. Then $u\pi = \overline{u}\pi$ and since $\overline{u} \in \overline{L}$ would imply

$$u\pi = \overline{u}\pi \in \overline{L}\pi = L\pi = A,$$

we must have $\overline{u} \in \overline{X^*} \setminus \overline{L}$ and so $u\pi \in (\overline{X^*} \setminus \overline{L})\pi$.

Conversely, assume that $u \in \overline{X^*} \setminus \overline{L}$. Since $u\pi \in A = L\pi$ yields $u = \overline{u} \in \overline{L}$, a contradiction, we conclude that $u\pi \in M \setminus A$ and so (1) holds.

Since $\overline{X^*} \setminus \overline{L} \in \operatorname{Rat} X^*$ by Theorem 3.1, it follows that $M \setminus A \in \operatorname{Rat} M$ and so $\operatorname{Rat} M$ is closed under complementation as required. $\square$

If we consider the whole reduction class, we are taken into the realm of deterministic context-free languages. By [9, Lemma 3.6], the result proved by Chottin [5] for finite length-reducing left basic confluent rewriting systems can be immediately generalized to the rational case:

Theorem 3.4 (*[5,9]*). *Let $\mathcal{R}$ be a rational length-reducing left basic confluent rewriting system on a finite alphabet X. Let $M = X^*/\mathcal{R}^\sharp$ and let $\pi : X^* \to M$ be the canonical homomorphism. For every $L \in \operatorname{Rat} X^*$, $L\pi\pi^{-1}$ is an effectively constructible deterministic context-free language.*

This constitutes a generalization of the result proved by Sakarovitch in 1979 for finite L [7, Theorem 7.6].

We can now obtain decidability for recognizability:

Corollary 3.5. *Let $\mathcal{R}$ be a rational length-reducing left basic confluent rewriting system on a finite alphabet X and let $M = X^*/\mathcal{R}^\sharp$. Then it is decidable whether or not a given $A \in \operatorname{Rat} M$ is recognizable.*

Proof. Let $\pi : X^* \to M$ be the canonical homomorphism. We know that $A = L\pi$ for some $L \in \operatorname{Rat} X^*$ and L can be effectively computed from A. By Theorem 3.4, $L\pi\pi^{-1}$ is an effectively constructible deterministic context-free language and so, by [6, Th. 10.6], it is decidable whether or not $L\pi\pi^{-1} \in \operatorname{Rec} X^*$. Since

$$L\pi\pi^{-1} \in \operatorname{Rec} X^* \Leftrightarrow L\pi \in \operatorname{Rec} M$$

by Lemma 2.1, it is decidable whether or not $A = L\pi \in \operatorname{Rec} M$. $\square$

Our attention was called to the fact that results of Sénizergues [8,11,12] may be used and adapted to prove that the syntactic monoids of rational languages have a decidable word problem in the general case of monoids defined by rational length-reducing left basic confluent rewriting systems. Among those results, we may need in the more general cases the decidability of the equivalence problem for deterministic pushdown automata [12]. The complexity of this latter algorithm is double exponential [15]. In Section 4, we shall give an elementary proof for the restricted case of PR-monoids that is fully automata-theoretic and has lower complexity.

4. PR-monoids: Syntactic monoids of rational subsets

Formally, a *partially reversible* monoid (PR-monoid) is the monoid defined by a finite monoid presentation $\mathrm{Mon}\langle X \mid R\rangle$, where

$$X = X_0 \cup X_1^{\pm 1} \cup X_2^{\pm 1} \tag{2}$$

is a disjoint union and

$$R = \{xx^{-1} = 1 \mid x \in X_1 \cup X_2^{\pm 1}\}. \tag{3}$$

If $X_1 = \emptyset$, the corresponding PR-monoid is said to be *strict*. It is easy to see that a PR-monoid is strict if and only if every left invertible element is invertible.

Proposition 4.1. *Every PR-monoid admits a finite special confluent rewriting system.*

Proof. Let M be the PR-monoid defined by the finite monoid presentation $\mathrm{Mon}\langle X \mid R\rangle$ described by (2) and (3).

We consider the rewriting system on X defined by

$$\mathcal{R} = \{xx^{-1} \to 1,\ x \in X_1 \cup X_2^{\pm 1}\}. \tag{4}$$

The rewriting system $\mathcal{R}$ is obviously finite and special. The proof for (local) confluence is straightforward and can be omitted. □

For the remaining part of this section, we assume that M is the PR-monoid defined by the finite rewriting system (4) on X. Keeping the notation used in Section 2, we denote by $\pi : X^* \to M$ the canonical homomorphism and we denote by $\overline{u}$ the unique irreducible word equivalent to $u \in X^*$.

We define a relation on $\overline{X^*} \times \overline{X^*}$ by:

$$(u, v) \longrightarrow (u', v')$$

if there exists some $x \in X_1 \cup X_2^{\pm 1}$ such that one of the following conditions holds:

(C1) $u = x^{-1}u'$ and $v' = \overline{xv}$;
(C2) $u' = \overline{xu}$ and $v = x^{-1}v'$;
(C3) $u = u'x$ and $v' = \overline{vx^{-1}}$;
(C4) $u' = \overline{ux^{-1}}$ and $v = v'x$.

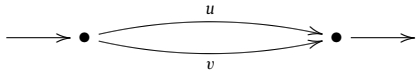
We denote by $\xrightarrow{*}$ the reflexive and transitive closure of $\longrightarrow$ and we write

$$\mathrm{Conj}(u, v) = \{(u', v') \in \overline{X^*} \times \overline{X^*} \mid (u, v) \xrightarrow{*} (u', v')\}.$$

Since $(u, v) \to (u', v')$ implies $|u'| + |v'| \leq |u| + |v|$, the set $\mathrm{Conj}(u, v)$ is finite and can be effectively computed. In fact, we have:

Lemma 4.2. *For all* $u, v \in \overline{X^*} \times \overline{X^*}$, $|\mathrm{Conj}(u, v)| \leq |uv|^2 + |uv|$.

Proof. We can build an automaton $\mathcal{B}$ with $|uv|$ vertices of the form



where for simplicity we assume every edge $p \xrightarrow{x} q$ to have a formal dual edge $q \xrightarrow{x^{-1}} p$ for every $x \in X$ (i.e, even if $x \in X_0$). For every vertex p in $\mathcal{B}$ and $j \in \{0, |uv|\}$, let $g_{p,j}$ (respectively $h_{p,j}$) be the label of the clockwise (respectively anticlockwise) path of length j starting at p.

We claim that, for every $(u', v') \in \mathrm{Conj}(u, v)$, there exists a vertex p in $\mathcal{B}$ and $j \in \{0, |uv|\}$ such that

$$g_{p,j}, h_{p,|uv|-j} \in X^*, \quad u' = \overline{g_{p,j}}, \quad v' = \overline{h_{p,|uv|-j}}. \tag{5}$$

We proceed by induction. Clearly, (5) holds for $(u, v) \in \mathrm{Conj}(u, v)$ taking p as the initial vertex and $j = |u|$. Assume now that (5) holds for $(u', v') \in \mathrm{Conj}(u, v)$ and assume that $(u', v') \longrightarrow (u'', v'')$. We suppose first that (u'', v'') is obtained through (C1). Hence there exists some $x \in X_1 \cup X_2^{\pm 1}$ such that $u' = x^{-1}u''$ and $v'' = \overline{xv'}$. Since $\overline{g_{p,j}} = x^{-1}u''$, we may write $g_{p,j} = wx^{-1}z$ with $\overline{w} = 1$ and $\overline{z} = u''$. Let q be the vertex obtained by reading wx^{-1} from p clockwise and let $k = j - |w| - 1 \geq 0$. Since

$g_{p,j} = wx^{-1}g_{q,k}$, we have $g_{q,k} \in X^*$. On the other hand, $h_{q,|uv|-k} = xw^{-1}h_{p,|uv|-j}$. Now $x \in X_1 \cup X_2^{\pm 1}$, and $\overline{w} = 1$ implies $w \in X_1^{\pm 1} \cup X_2^{\pm 1}$, thus $h_{q,|uv|-k} \in X^*$ as well.

Since $\overline{w} = 1$ yields $\overline{w^{-1}} = 1$, it follows that

$$x^{-1}u'' = u' = \overline{g_{p,j}} = \overline{wx^{-1}g_{q,k}} = \overline{x^{-1}g_{q,k}}$$

and so $\overline{g_{q,k}} = \overline{xx^{-1}u''} = u''$. Finally,

$$\overline{h_{q,|uv|-k}} = \overline{xw^{-1}h_{p,|uv|-j}} = \overline{xv'} = v''$$

and so (5) holds for (u'', v'').

Suppose now that (u'', v'') is obtained through (C2). Hence there exists some $x \in X_1 \cup X_2^{\pm 1}$ such that $u'' = \overline{xu'}$ and $v' = x^{-1}v''$. Since $\overline{h_{p,|uv|-j}} = x^{-1}v''$, we may write $h_{p,|uv|-j} = wx^{-1}z$ with $\overline{w} = 1$ and $\overline{z} = v''$. Let q be the vertex obtained by reading wx^{-1} from p anticlockwise and let $k = j + |w| + 1$. Since $|w| + 1 \leq |uv| - j$, we have $k \leq |uv|$. Similarly to the preceding case, the equalities $g_{q,k} = xw^{-1}g_{p,j}$ and $h_{p,|uv|-j} = wx^{-1}h_{q,|uv|-k}$ yield the claim. We omit the proofs for the cases (C3) and (C4).

Therefore (5) holds. Since $\mathcal{B}$ has $|uv|$ vertices, we get $|\mathrm{Conj}(u, v)| \leq |uv|(|uv| + 1)$ and the lemma is proved. □

Lemma 4.3. *Let $A \subseteq M$ and $u, v \in \overline{X^*}$. If $(u', v') \in \mathrm{Conj}(u, v)$, then*

$$u\pi \sim_A v\pi \Rightarrow u'\pi \sim_A v'\pi.$$

Proof. We may assume that $(u, v) \longrightarrow (u', v')$. Then one of the conditions (C1)–(C4) must be satisfied for some $x \in X_1 \cup X_2^{\pm 1}$. Since $(xx^{-1})\pi = 1\pi$, we have in cases (C1) and (C2) $u'\pi = (xu)\pi$ and $v'\pi = (xv)\pi$. In cases (C3) and (C4) we have $u'\pi = (ux^{-1})\pi$ and $v'\pi = (vx^{-1})\pi$. In any case, $u\pi \sim_A v\pi$ implies $u'\pi \sim_A v'\pi$ since $\sim_A$ is a congruence. □

Theorem 4.4. *Let $A \in \mathrm{Rat}\, M$. Then the syntactic monoid $M/\sim_A$ has a decidable word problem.*

Proof. Write $A = L\pi$ for some $L \in \mathrm{Rat}\, X^*$. Since $L\pi = \overline{L}\pi$, we may assume that $L = \overline{L}$ by Theorem 3.1. By Lemma 2.2, there exists a finite deterministic accessible X-automaton $\mathcal{A} = (Q, i, T, E)$ such that $L(\mathcal{A}) = L$ and $L_{in}(\mathcal{A}) = \overline{X^*}$.

Let $u, v \in \overline{X^*}$. We show that $(u\pi, v\pi) \notin \sim_A$ if and only if there exist $(w, z) \in \mathrm{Conj}(u, v)$, $a, b \in \overline{X^*}$ and $p \in (X_1 \cup X_2^{\pm 1})^*$ such that one of the following conditions holds:

(D1) $awb \in L, azb \in \overline{X^*} \setminus L$;
(D1′) $awb \in \overline{X^*} \setminus L, azb \in L$;
(D2) $z = 1, apwp^{-1}b \in L, ab \in \overline{X^*} \setminus L$;
(D2′) $w = 1, apzp^{-1}b \in L, ab \in \overline{X^*} \setminus L$;
(D3) $z = 1, apwp^{-1}b \in \overline{X^*} \setminus L, ab \in L$;
(D3′) $w = 1, apzp^{-1}b \in \overline{X^*} \setminus L, ab \in L$.

Intuitively, we want to consider simultaneously the reduction process of words aub, avb. The basic idea is that reduction in single steps produces pairs of words $a'u'b'$, $a'v'b'$ with $(u', v') \in \mathrm{Conj}(u, v)$ and therefore only finitely many words u', v' can be thus obtained. Pursuing the reduction process until the end, we claim that we fall necessarily within one of the cases (D1)–(D3′).

Assume first that (D1) holds. Then $(awb)\pi \in L\pi = A$. Since $L \subseteq \overline{X^*}$, we have $\overline{azb} \notin \overline{L}$ and so $(azb)\pi \notin A$. Thus $(w\pi, z\pi) \notin \sim_A$ and so $(u\pi, v\pi) \notin \sim_A$ by Lemma 4.3.

Assume now that (D2) holds. Then $(apwp^{-1}b)\pi \in A$ and $\overline{ab} \notin \overline{L}$ yields $(app^{-1}b)\pi \notin A$. Thus $(w\pi, z\pi) = (w\pi, 1\pi) \notin \sim_A$ and so $(u\pi, v\pi) \notin \sim_A$ by Lemma 4.3.

The dual cases (D1′), (D2′), (D3) and (D3′) are absolutely similar.

Conversely, assume that $(u\pi, v\pi) \notin \sim_A$. Then there exist $a, b \in \overline{X^*}$ such that $(aub)\pi \in A$ and $(avb)\pi \notin A$ or vice versa. We use induction on $|aub| + |avb| = k$, assuming that, for all $u', v', a', b' \in \overline{X^*}$ such that:

- $(a'u'b')\pi \in A$ and $(a'v'b')\pi \notin A$ or vice versa;
- $|a'u'b'| + |a'v'b'| < k$;

there exist $(w, z) \in \mathrm{Conj}(u', v')$, $a'', b'' \in \overline{X^*}$ and $p \in (X_1 \cup X_2^{\pm 1})^*$ such that one of the conditions (D1)–(D3′) holds.

Without loss of generality, we may assume that $(aub)\pi \in A$ and $(avb)\pi \notin A$, the opposite case being treated symmetrically. Hence $\overline{aub} \in L$ and $\overline{avb} \notin L$. If $aub, avb \in \overline{X^*}$, then (D1) holds for $(w, z) = (u, v)$ trivially, hence we assume that at least one of the words aub, avb is not irreducible.

Case A: $au \notin \overline{X^*}$.

Then we may write $a = a'x$, $u = x^{-1}u'$ for some $x \in X_1 \cup X_2^{\pm 1}$. Hence

$$(a'u'b)\pi = (aub)\pi \in A, \quad (a'\overline{xv}b)\pi = (a'xvb)\pi = (avb)\pi \notin A.$$

Since $|a'u'b| + |a'\overline{xv}b| < k$, we may apply the induction hypothesis and conclude that there exist $(w, z) \in \mathrm{Conj}(u', \overline{xv})$; $a'', b'' \in \overline{X^*}$ and $p \in (X_1 \cup X_2^{\pm 1})^*$ such that one of the conditions (D1)–(D3′) holds. Since $(u, v) \to (u', \overline{xv})$ by (C1), we have $(w, z) \in \mathrm{Conj}(u, v)$ and so the lemma holds for u, v in this case.

Case B: $av \notin \overline{X^*}$.

This case is symmetric to Case A.

Case C: $ub \notin \overline{X^*}$.

Then we may write $u = u'x$, $b = x^{-1}b'$ for some $x \in X_1 \cup X_2^{\pm 1}$. Hence

$$(au'b')\pi = (aub)\pi \in A, \quad (a\overline{vx^{-1}}b')\pi = (avx^{-1}b')\pi = (avb)\pi \notin A.$$

Similarly to Case A, there exist $(w, z) \in \mathrm{Conj}(u', \overline{vx^{-1}})$; $a'', b'' \in \overline{X^*}$ and $p \in (X_1 \cup X_2^{\pm 1})^*$ such that one of the conditions (D1)–(D3′) holds, and $(u, v) \to (u', \overline{vx^{-1}})$ by (C3) yields $(w, z) \in \mathrm{Conj}(u, v)$.

Case D: $vb \notin \overline{X^*}$.

This case is symmetric to Case C.

Having proved Cases A–D, we suppose that $u, v \neq 1$. Since $aub \notin \overline{X^*}$ or $avb \notin \overline{X^*}$, we fall necessarily into one of the cases A–D.

Suppose now that $u = 1$. Then $v \neq 1$, and $avb \notin \overline{X^*}$ takes us into cases C or D, hence we may assume that $avb \in \overline{X^*}$. Hence $ab \notin \overline{X^*}$. Since a and b are irreducible, we must have $a = a'p$, $b = p^{-1}b'$ for some $p \in (X_1 \cup X_2^{\pm 1})^*$ with $\overline{ab} = a'b'$. Therefore

$$(a'pvp^{-1}b')\pi = (avb)\pi \notin A, \quad (a'b')\pi = (a'pup^{-1}b')\pi = (aub)\pi \in A$$

and so

$$a'pvp^{-1}b' \in \overline{X^*} \setminus L, \quad a'b' \in L.$$

Therefore (D3′) holds for $(w, z) = (u, v)$, a', b' and p.

The case $v = 1$ is symmetric.

Therefore we proved that $(u\pi, v\pi) \notin \sim_A$ if and only if there exist $(w, z) \in \mathrm{Conj}(u, v)$; $a, b \in \overline{X^*}$ and $p \in (X_1 \cup X_2^{\pm 1})^*$ such that one of the conditions (D1)–(D3′) holds. We prove that each one of these conditions is decidable. Since $\mathrm{Conj}(u, v)$ is a finite computable set, we may assume that w, z are fixed.

For all $q, q' \in Q$, write $L_{qq'} = L(Q, q, q', E)$. We show that condition (D1) holds if and only if there exist $q_1, q_2, q_3, q_4, q_5 \in Q$ such that:

(D1a) $w \in L_{q_1q_2}, z \in L_{q_1q_4}$;
(D1b) $L_{q_2q_3} \cap L_{q_4q_5} \neq \emptyset$;
(D1c) $q_3 \in T, q_5 \notin T$.

In fact, if these conditions hold, we take $a \in L_{iq_1}$ (nonempty since $\mathcal{A}$ is accessible) and $b \in L_{q_2q_3} \cap L_{q_4q_5}$. Then $awb \in L_{iq_3} \subseteq L(\mathcal{A}) = L$ and $azb \in L_{iq_5} \subseteq L_{in}(\mathcal{A}) \setminus L(\mathcal{A}) = \overline{X^*} \setminus L$, and (D1) holds.

Conversely, if (D1) holds for (w, z), we have paths in $\mathcal{A}$ of the form

$$i \xrightarrow{a} q_1 \xrightarrow{w} q_2 \xrightarrow{b} q_3 \in T,$$
$$i \xrightarrow{a} q_1 \xrightarrow{z} q_4 \xrightarrow{b} q_5 \notin T,$$

the existence of the last path following from $L_{in}(\mathcal{A}) = \overline{X^*}$. Thus conditions (D1a)–(D1c) hold for q_1, q_2, q_3, q_4, q_5.

Since conditions (D1a)–(D1c) are clearly decidable for every possible choice of $q_1, q_2, q_3, q_4, q_5 \in Q$, we conclude that condition (D1) is decidable.

Next we show that condition (D2) holds if and only if $z = 1$ and there exist $q_1, q_2, q_3, q_4, q_5, q_6 \in Q$ such that:

(D2a) $w \in L_{q_2q_3}$;
(D2b) $L_{q_1q_6} \cap L_{q_4q_5} \neq \emptyset$;
(D2c) $L_{q_1q_2} \cap (L_{q_3q_4})^{-1} \cap (X_1 \cup X_2^{\pm 1})^* \neq \emptyset$;
(D2d) $q_5 \in T, q_6 \notin T$.

If these conditions hold, we take $a \in L_{iq_1}$ (nonempty since $\mathcal{A}$ is accessible), $b \in L_{q_1q_6} \cap L_{q_4q_5}$ and

$$p \in L_{q_1q_2} \cap (L_{q_3q_4})^{-1} \cap (X_1 \cup X_2^{\pm 1})^* \neq \emptyset.$$

Then $apwp^{-1}b \in L_{iq_5} \subseteq L$ and $ab \in L_{iq_6} \subseteq \overline{X^*} \setminus L$, and (D2) holds.

Conversely, if (D2) holds for (w, z), then $z = 1$ and we have paths in $\mathcal{A}$ of the form

$$i \xrightarrow{a} q_1 \xrightarrow{p} q_2 \xrightarrow{w} q_3 \xrightarrow{p^{-1}} q_4 \xrightarrow{b} q_5 \in T,$$
$$i \xrightarrow{a} q_1 \xrightarrow{b} q_6 \notin T,$$

with $p \in (X_1 \cup X_2^{\pm 1})^*$. Thus conditions (D2a)–(D2d) hold for $q_1, q_2, q_3, q_4, q_5, q_6$.

Note that, given $P \in \operatorname{Rat} X^*$, P^{-1} is an effectively constructible rational language (follows easily from the class of rational languages being closed under reversal and homomorphic images). Therefore conditions (D2a)–(D2d) are decidable for every possible choice of $q_1, q_2, q_3, q_4, q_5, q_6 \in Q$ and we conclude that condition (D2) is decidable.

Decidability of the remaining conditions follows by duality, thus we can decide whether or not $(u\pi, v\pi) \notin \sim_A$ for all $u, v \in \overline{X}^*$. Since

$$(u\pi, v\pi) \in \sim_A \Leftrightarrow (\overline{u}\pi, \overline{v}\pi) \in \sim_A$$

for all $u, v \in X^*$, the word problem for the syntactic monoid $M/\sim_A$ is therefore decidable. □

Corollary 4.5. *Let $A \in \operatorname{Rat} M$ and let n be the number of vertices of $\min_{\overline{A}}$. For all $u, v \in X^*$, $u \sim_A v$ is decidable with polynomial complexity with respect to $n + |X| + |uv|$.*

Proof. First, note that $u \sim_A v$ if and only if $\overline{u} \sim_A \overline{v}$. Let us apply the construction of Lemma 2.2 as in the proof of Theorem 4.4. We can turn $\min_{\overline{A}}$ into a complete deterministic automaton by adding a sink vertex. It is a simple exercise to show that the minimal automaton of $\overline{X^*}$ has at most $|X| + 1$ vertices, hence the finite deterministic accessible X-automaton $\mathcal{A}$ has at most $(n + 1)(|X| + 1)$ vertices [2] and its construction involves a polynomial number of steps. Now, given $u, v \in X^*$, it follows from Lemma 4.2 that $\operatorname{Conj}(\overline{u}, \overline{v})$ has at most $|\overline{u}\,\overline{v}|^2 + |\overline{u}\,\overline{v}|$ elements, and the number of steps involved in its computation is certainly polynomial on $|X| + |uv|$. Hence it is enough to show that deciding each one of the conditions (D1)–(D3′) for a fixed $(w, z) \in \operatorname{Conj}(\overline{u}, \overline{v})$ has the claimed polynomial complexity.

Without loss of generality, we may restrict our attention to (D2). It follows easily that all conditions (D2a)–(D2d) can be easily checked in the direct product $\mathcal{A} \times \mathcal{A}$, that has at most $(n+1)^2(|X|+1)^2$ vertices, involving only a polynomial number of steps. □

Note that the computation of $\min_{\overline{A}}$ may involve exponential complexity, but combination of single exponential with polynomial complexity is still better than double exponential.

5. PR-monoids: Recognizability

Keeping the notation of the preceding section, we assume that $\pi : X^* \to M$ is the canonical homomorphism onto the PR-monoid defined by (4), and we denote by $\overline{u}$ the unique irreducible word equivalent to $u \in X^*$.

We introduce a strict PR-monoid associated to M. Let $\mathcal{R}'$ denote the rewriting system on X defined by

$$\mathcal{R}' = \{xx^{-1} \to 1,\ x \in X_1^{\pm 1} \cup X_2^{\pm 1}\}.$$

Let $M' = X^*/\mathcal{R}'^{\sharp}$. We denote by $\pi' : X^* \to M'$ the canonical homomorphism and we denote by $\widetilde{u}$ the unique irreducible word equivalent to $u \in X^*$ modulo $\mathcal{R}'^{\sharp}$.

Lemma 5.1. *Let $L \in \operatorname{Rat} X^*$ be such that $((x^{-1}x)\pi, 1\pi) \in \sim_{L\pi}$ for every $x \in X_1$. Then $L\pi\pi^{-1} = L\pi'\pi'^{-1}$.*

Proof. Since $\mathcal{R} \subseteq \mathcal{R}'$, we have $\mathcal{R}^{\sharp} \subseteq \mathcal{R}'^{\sharp}$ and so

$$L\pi\pi^{-1} = L\mathcal{R}^{\sharp} \subseteq L\mathcal{R}'^{\sharp} = L\pi'\pi'^{-1}.$$

Conversely, let $u \in L\pi'\pi'^{-1} = L\mathcal{R}'^{\sharp}$. By the definition of congruence generated by a relation, u is obtained from some $v \in L$ by successively inserting/deleting factors of the form yy^{-1}, with $y \in X_1^{\pm 1} \cup X_2^{\pm 1}$. Since $((x^{-1}x)\pi, 1\pi) \in \sim_{L\pi}$ for every $x \in X_1$, Lemma 2.1 yields $(x^{-1}x, 1) \in \sim_{L\pi\pi^{-1}}$ for every $x \in X_1$ and so we actually have $(yy^{-1}, 1) \in \sim_{L\pi\pi^{-1}}$ for every $y \in X_1^{\pm 1} \cup X_2^{\pm 1}$. Therefore $L\pi\pi^{-1}$ is closed under inserting/deleting factors of the form yy^{-1}. Since $v \in L \subseteq L\pi\pi^{-1}$, we conclude in particular that $u \in L\pi\pi^{-1}$. Therefore $L\pi'\pi'^{-1} \subseteq L\pi\pi^{-1}$ and so equality holds. □

Theorem 5.2. *Let $L \in \operatorname{Rat} X^*$. Then $L\pi \in \operatorname{Rec} M$ if and only if the following conditions hold:*

(i) $L\pi' \in \operatorname{Rec} M'$;
(ii) $((x^{-1}x)\pi, 1\pi) \in \sim_{L\pi}$ *for every* $x \in X_1$.

Proof. By Lemma 2.1, we have $L\pi \in \operatorname{Rec} M$ (respectively $L\pi' \in \operatorname{Rec} M'$) if and only if $L\pi\pi^{-1} \in \operatorname{Rat} X^*$ (respectively $L\pi'\pi'^{-1} \in \operatorname{Rat} X^*$). Therefore, by Lemma 5.1, it suffices to show that $L\pi \in \operatorname{Rec} M$ implies condition (ii), since the latter yields $L\pi\pi^{-1} = L\pi'\pi'^{-1}$.

Assume that $L\pi \in \operatorname{Rec} M$ and let $x \in X_1$. Since $\sigma = \sim_{L\pi}$ has finite index, there exist $m, n > 0$ such that $x^n\pi\sigma = x^{n+m}\pi\sigma$. Thus

$$\begin{aligned}(x^{-1}x)\pi\sigma &= (x^n x^{-n-1}x)\pi\sigma = (x^{n+m}x^{-n-1}x)\pi\sigma = x^m\pi\sigma \\ &= (x^m x^n x^{-n})\pi\sigma = (x^n x^{-n})\pi\sigma = 1\pi\sigma\end{aligned}$$

as required. □

In view of Theorem 4.4, the preceding result reduces the characterization of recognizable subsets of PR-monoids to the characterization of recognizable subsets of strict PR-monoids. In particular, if $X_0 = \emptyset$, we reduce our problem to the characterization of recognizable subsets of the free group. This is not too surprising taking into account the well-known fact that finite (cyclic) groups are the unique finite quotients of the bicyclic monoid.

Lemma 5.3. *Let $L \in \operatorname{Rat} X^*$ be nonempty and such that $L\pi \in \operatorname{Rec} M$. Let $\mathcal{A} = \min_{L\pi\pi^{-1}} = (Q, i, T, E)$. Then:*

(i) *for all $x \in X_1^{\pm 1} \cup X_2^{\pm 1}$ and $p \in Q$, $(p, x, q) \in E$ for some $q \in Q$;*
(ii) *for all $x \in X_1^{\pm 1} \cup X_2^{\pm 1}$ and $p, q \in Q$,*

$$(p, x, q) \in E \Rightarrow (q, x^{-1}, p) \in E.$$

Proof. (i) Let $x \in X_1^{\pm 1} \cup X_2^{\pm 1}$ and $p \in Q$. Since $\mathcal{A}$ is trim, we have a path

$$i \xrightarrow{u} p \xrightarrow{v} t \in T.$$

Since $L\pi \in \operatorname{Rec} M$, we have $((y^{-1}y)\pi, 1\pi) \in \sim_{L\pi}$ for every $y \in X_1$ by Theorem 5.2, hence $L\pi\pi^{-1} = L\pi'\pi'^{-1}$ by Lemma 5.1 and so $L(\mathcal{A}) = L\pi'\pi'^{-1}$. In particular, $uv \in L(\mathcal{A}) = L\pi'\pi'^{-1}$. It follows that $(uxx^{-1}v)\pi' = (uv)\pi' \in L\pi'$ and so $uxx^{-1}v \in L\pi'\pi'^{-1} = L(\mathcal{A})$. Since $\mathcal{A}$ is deterministic, this implies $(p, x, q) \in E$ for some $q \in Q$.

(ii) Suppose that there exist $x \in X_1^{\pm 1} \cup X_2^{\pm 1}$ and $p, q \in Q$ such that

$$(p, x, q) \in E, \quad (q, x^{-1}, p) \notin E.$$

By (i), we have $(q, x^{-1}, r) \in E$ for some $r \in Q$. Since $r \neq p$ and $\mathcal{A}$ is minimal, there exists some $v \in X^*$ such that one of the following four situations holds:

- there exist paths of the form $p \xrightarrow{v} t \in T$, $r \xrightarrow{v} s \notin T$;
- there exists a path of the form $p \xrightarrow{v} t \in T$ and rv is undefined;
- there exist paths of the form $p \xrightarrow{v} s \notin T$, $r \xrightarrow{v} t \in T$;
- there exists a path of the form $r \xrightarrow{v} t \in T$ and pv is undefined.

Fix a path $i \xrightarrow{u} p$. Then we have either

$$uv \in L(\mathcal{A}), \quad uxx^{-1}v \notin L(\mathcal{A})$$

or

$$uv \notin L(\mathcal{A}), \quad uxx^{-1}v \in L(\mathcal{A}).$$

Since we observed in part (i) that $L(\mathcal{A}) = L\pi'\pi'^{-1}$, the equivalence

$$uv \in L\pi'\pi'^{-1} \Leftrightarrow uxx^{-1}v \in L\pi'\pi'^{-1}$$

does not hold. Since $(uv)\pi' = (uxx^{-1}v)\pi'$, we reach a contradiction. Therefore (ii) holds. □

Lemma 5.4. *Suppose that M is strict. Let $L \in \operatorname{Rat} X^*$ be nonempty and such that $L\pi \in \operatorname{Rec} M$. Let $\mathcal{A} = \min_{L\pi\pi^{-1}}$. Then*

$$\min_{\overline{L}} = \operatorname{acc}(\mathcal{A} \times \min_{\overline{X^*}}).$$

Proof. Write $\mathcal{A} = (Q, i, T, E)$, $\min_{\overline{X^*}} = (Q', i', T', E')$ and $\mathcal{B} = \operatorname{acc}(\mathcal{A} \times \min_{\overline{X^*}})$. Clearly,

$$L(\mathcal{B}) = L(\mathcal{A} \times \min_{\overline{X^*}}) = L(\mathcal{A}) \cap L(\min_{\overline{X^*}}) = L\pi\pi^{-1} \cap \overline{X^*} = \overline{L}.$$

Moreover, $\mathcal{B}$ is an accessible deterministic X-automaton. We show that it is also co-accessible and therefore trim.

Let $(p, p') \in Q \times Q'$ be a state of $\mathcal{B}$. Then there exists a path in $\mathcal{B}$ of the form

$$(i, i') \xrightarrow{u} (p, p').$$

In particular, we have a path

$$i \xrightarrow{u} p$$

in $\mathcal{A}$. Note that, since $\mathcal{A}$ is deterministic, we may conclude from Lemma 5.3 that

$$r \xrightarrow{ab} s \Leftrightarrow r \xrightarrow{axx^{-1}b} s$$

holds in $\mathcal{A}$ for all $r, s \in Q$; $a, b \in X^*$ and $x \in X_2^{\pm 1}$. Therefore

$$r \xrightarrow{w} s \Leftrightarrow r \xrightarrow{\overline{w}} s \tag{6}$$

holds in $\mathcal{A}$ for all $r, s \in Q$ and $w \in X^*$.

Suppose first that $u = u'x$ for some $u' \in X^*$ and $x \in X_2^{\pm 1}$. By Lemma 5.3(i), we have a path of the form

$$p \xrightarrow{x^n} q$$

in $\mathcal{A}$ for $n = |Q|$. Since $\mathcal{A}$ is trim, we also have a path

$$q \xrightarrow{v} t \in T$$

in $\mathcal{A}$ for some $v \in X^*$ satisfying $|v| < n$. Thus $ux^n v \in L(\mathcal{A}) = L\pi\pi^{-1}$ and so $\overline{ux^n v} \in L(\mathcal{A})$. Since u labels a path in $\min_{\overline{X^*}}$, we have $u \in \overline{X^*}$ and so $ux^n = u'x^{n+1} \in \overline{X^*}$. Since $|v| < n$, we conclude that

$$u\overline{x^n v} = \overline{ux^n v} \in L(\mathcal{A}) \cap \overline{X^*} = L(\mathcal{B}).$$

Hence (p, p') is co-accessible as required.

Finally, suppose that $u \notin X^*X_2^{\pm 1}$. Since $\mathcal{A}$ is trim, we must have a path of the form

$$p \xrightarrow{v} t \in T$$

in $\mathcal{A}$. By (6), we may assume that $v \in \overline{X^*}$. Since $u, v \in \overline{X^*}$ and $u \notin X^*X_2^{\pm 1}$, it follows that $uv \in \overline{X^*}$. Then we have a path of the form

$$p' \xrightarrow{v} t' \in T'$$

in $\min_{\overline{X^*}}$ and so there is a path

$$(p, p') \xrightarrow{v} (t, t') \in T \times T'$$

in $\mathcal{B}$. Thus $\mathcal{B}$ is accessible and therefore trim.

To show that $\mathcal{B}$ is minimal, it remains to prove that any two distinct states (p, p'), (q, q') of $\mathcal{B}$ can be distinguished by paths into terminal states. Since $\mathcal{B}$ is accessible, we have paths of the form

$$(i, i') \xrightarrow{u} (p, p'), \quad (i, i') \xrightarrow{v} (q, q')$$

in $\mathcal{B}$. In particular, $u, v \in \overline{X^*}$.

Suppose first that $p' \neq q'$. Without loss of generality, we may assume that $p'w \in T'$ and $q'w \notin T'$ for some $w \in X^*$. Since $p'w \in T'$ yields $uw \in \overline{X^*}$, we obtain $w \in \overline{X^*}$ and from $q'w \notin T'$ we conclude that $vw \notin \overline{X^*}$. This implies that $v = v'x$, $w = x^{-1}w'$ for some $x \in X_2^{\pm 1}$, hence $p'x^{-1} \neq \emptyset$ and $q'x^{-1} = \emptyset$. On the one hand, we have by Lemma 5.3(i) a path of the form

$$p \xrightarrow{x^{-1}} r$$

in $\mathcal{A}$ and so there is a path

$$(p, p') \xrightarrow{x^{-1}} (r, r')$$

in $\mathcal{B}$ (since (p, p') is accessible, (r, r') is accessible). Since we have already proved that $\mathcal{B}$ is trim, we may extend this path into some terminal state by

$$(r, r') \xrightarrow{z} (t, t') \in T \times T'.$$

On the other hand, $q'x^{-1} = \emptyset$ in $\min_{\overline{X^*}}$ implies $(q, q')x^{-1}z = \emptyset$ in $\mathcal{B}$ and so (p, p'), (q, q') can be distinguished by paths into terminal states.

Finally, assume that $p' = q'$ and $p \neq q$. Without loss of generality, we may assume that $pw = t \in T$ and $qw \notin T$ for some $w \in X^*$. By (6), we may assume that $w \in \overline{X^*}$.

Suppose first that $uw \in \overline{X^*}$. Then $p'w \in T'$ and so $(p, p')w \in T \times T'$ and $(q, q')w \notin T \times T'$ as required. Assume now that $uw \notin \overline{X^*}$. Then we may write $u = u'x$, $w = x^{-1}w'$ for some $x \in X_2^{\pm 1}$. By Lemma 5.3(i), we have a path $p \xrightarrow{x^n} r$ in $\mathcal{A}$ for $n = |Q|$. Since $n = |Q|$ and $\mathcal{A}$ is deterministic, we may factor this path as

$$p \xrightarrow{x^{n_1}} r \xrightarrow{x^{n_2}} r$$

with $n_2 > 0$. In view of Lemma 5.3(ii), $\mathcal{A}$ is codeterministic and so the vertex p must occur somewhere in the loop $r \xrightarrow{x^{n_2}} r$. It follows that there is a loop $p \xrightarrow{x^m} p$ with $m > |w|$. The same argument can be of course applied to state q, and taking a common multiple if necessary we may assume that x^m labels a loop at state q as well.

Hence we have a path in $\mathcal{A}$ given by

$$i \xrightarrow{u} p \xrightarrow{x^m} p \xrightarrow{w} t \in T$$

and so $ux^m w \in L(\mathcal{A})$. Since $m > |w|$ and $u = u'x$, we get $\overline{ux^m w} = u\overline{x^m w}$. By (6), we obtain a path

$$p \xrightarrow{\overline{x^m w}} t.$$

Since $u\overline{x^m w} \in \overline{X^*}$, we have $p'\overline{x^m w} \in T'$ and so $(p, p')\overline{x^m w} \in T \times T'$. On the other hand, $qx^m w = q\overline{x^m w} = qw \notin T$ since x^m labels a loop at q and in view of (6), we conclude that $(q, q')\overline{x^m w} \notin T \times T'$ and so (p, p'), (q, q') can be distinguished by paths into terminal states also in this final case.

Therefore $\mathcal{B}$ is minimal. □

Given an X-automaton $\mathcal{A} = (Q, i, T, E)$, define

$$D(\mathcal{A}) = (Q, i, T, D(E))$$

for

$$D(E) = E \cup \{(q, x^{-1}, p) \mid (p, x, q) \in E, x \in X_1^{\pm 1} \cup X_2^{\pm 1}\}.$$

This construction was introduced in [13] for the free group case.

Lemma 5.5. *Let $L \in \operatorname{Rat} X^*$ be nonempty and such that $L\pi \in \operatorname{Rec} M$ and let $\min_{\widetilde{L}} = (Q_0, i_0, T_0, E_0)$. Let $x \in X_1^{\pm 1} \cup X_2^{\pm 1}$ and $p \in Q_0$. Then $(p, x, q) \in D(E_0)$ for some $q \in Q_0$.*

Proof. Let $\mathcal{A} = (Q_1, i_1, T_1, E_1) = \min_{L\pi'\pi'^{-1}}$. By Lemma 5.4, we may write

$$\min_{\widetilde{L}} = \operatorname{acc}(\mathcal{A} \times \min_{\widetilde{X^*}}).$$

Let $\min_{\widetilde{X^*}} = (Q_2, i_2, T_2, E_2)$ and write $p = (p_1, p_2)$. Since p is accessible, we have a path $i_0 \xrightarrow{u} p$ in $\min_{\widetilde{L}}$ for some $u \in X^*$.

Assume first that $u \in X^*x^{-1}$. Then we have paths of the form

$$i_0 \xrightarrow{u'} p' \xrightarrow{x^{-1}} p$$

in $\min_{\widetilde{L}}$. Clearly, p' is accessible and $(p, x, p') \in D(E_0)$ as required.

Assume now that $u \notin X^*x^{-1}$. Then $ux \in \widetilde{X^*}$ and so there exists $q_2 \in Q_2$ such that $(p_2, x, q_2) \in E_2$.

On the other hand, by Theorem 5.2, we have $L\pi' \in \operatorname{Rec} M'$. Thus, by Lemma 5.3(i), there exists some $q_1 \in Q_1$ such that $(p_1, x, q_1) \in E_1$. Hence $(p, x, (q_1, q_2))$ is an edge of $\mathcal{A} \times \min_{\widetilde{X^*}}$. Since p is accessible, (q_1, q_2) is also accessible and so $(p, x, (q_1, q_2)) \in E_0$. □

Our next result generalizes [13, Th. 4.6], proved for the free group case.

Theorem 5.6. *Suppose that M is strict and let $L \in \operatorname{Rat} X^*$. Let $\min_{\overline{L}} = (Q_0, i_0, T_0, E_0)$. Then $L\pi \in \operatorname{Rec} M$ if and only if the following conditions hold:*

(i) *for all $x \in X_2^{\pm 1}$ and $p \in Q_0$, $(p, x, q) \in D(E_0)$ for some $q \in Q_0$;*
(ii) $\overline{L(D(\min_{\overline{L}}))} = \overline{L}$.

Proof. Assume first that $L\pi \in \operatorname{Rec} M$. Let $\mathcal{A} = (Q, i, T, E) = \min_{L\pi\pi^{-1}}$ and $\mathcal{A}' = (Q', i', T', E') = \min_{\overline{X^*}}$. Note that $\mathcal{A}$ is finite in view of Lemma 2.1. By Lemma 5.4, we may write $\min_{\overline{L}} = \operatorname{acc}(\mathcal{A} \times \mathcal{A}')$.

By Lemma 5.5, condition (i) holds.

Since $\overline{L} \subseteq L(D(\min_{\overline{L}}))$ trivially, we have

$$\overline{L} \subseteq \overline{L(D(\min_{\overline{L}}))}.$$

Conversely, let

$$(i, i') = (p_0, q_0) \xrightarrow{x_1} (p_1, q_1) \xrightarrow{x_2} \cdots \xrightarrow{x_n} (p_n, q_n) \in T \times T'$$

be a successful path in $D(\min_{\overline{L}}) = D(\operatorname{acc}(\mathcal{A} \times \mathcal{A}'))$. For every $j \in \{1, \ldots, n\}$, we have either

$$((p_{j-1}, q_{j-1}), x_j, (p_j, q_j)) \in E_0 \text{ or } ((p_j, q_j), x_j^{-1}, (p_{j-1}, q_{j-1})) \in E_0.$$

Thus $(p_{j-1}, x_j, p_j) \in E$ or $(p_j, x_j^{-1}, p_{j-1}) \in E$. By Lemma 5.3(ii), we obtain in any case $(p_{j-1}, x_j, p_j) \in E$ and so $x_1x_2 \ldots x_n \in L(\mathcal{A}) = L\pi\pi^{-1}$. Hence $L(D(\min_{\overline{L}})) \subseteq L\pi\pi^{-1}$ and so

$$\overline{L(D(\min_{\overline{L}}))} \subseteq \overline{L\pi\pi^{-1}} = \overline{L}.$$

Thus condition (ii) holds.

Conversely, assume that conditions (i) and (ii) hold. On the one hand, condition (ii) yields $(L(D(\min_{\overline{L}})))\pi = L\pi$ and so

$$L(D(\min_{\overline{L}})) \subseteq L\pi\pi^{-1}.$$

On the other hand, it follows from condition (i) that, for every $x \in X_2^{\pm 1}$, xx^{-1} labels a loop in $D(\min_{\overline{L}})$ at every vertex. Therefore, the implication

$$uv \in L(D(\min_{\overline{L}})) \Rightarrow uxx^{-1}v \in L(D(\min_{\overline{L}}))$$

holds for all $u, v \in X^*$ and $x \in X_2^{\pm 1}$. Since every word in $L\pi\pi^{-1}$ can be obtained from some word in $\overline{L} \subseteq L(D(\min_{\overline{L}}))$ by successively inserting factors of the form xx^{-1} ($x \in X_2^{\pm 1}$), we conclude that

$$L\pi\pi^{-1} \subseteq L(D(\min_{\overline{L}})).$$

Thus

$$L\pi\pi^{-1} = L(D(\min_{\overline{L}})) \in \operatorname{Rat} X^*$$

and so $L\pi \in \operatorname{Rec} M$ by Lemma 2.1. □

We can now generalize the preceding result to the nonstrict case:

Theorem 5.7. *Let $L \in \operatorname{Rat} X^*$ be nonempty and let $\min_{\widetilde{L}} = (Q_0, i_0, T_0, E_0)$. Then $L\pi \in \operatorname{Rec} M$ if and only if the following conditions hold:*

(i) *for all $x \in X_1^{\pm 1} \cup X_2^{\pm 1}$ and $p \in Q_0$, $(p, x, q) \in D(E_0)$ for some $q \in Q_0$;*
(ii) $L(\widetilde{D(\min_{\widetilde{L}})}) = \widetilde{L}$;
(iii) $((x^{-1}x)\pi, 1\pi) \in \sim_{L\pi}$ *for every $x \in X_1$.*

Proof. Assume that $L\pi \in \operatorname{Rec} M$. Condition (i) follows from Lemma 5.5. By Theorem 5.2, condition (iii) holds and $L\pi' \in \operatorname{Rec} M'$. Thus condition (ii) follows from Theorem 5.6.

Conversely, assume that conditions (i)–(iii) hold. By Theorem 5.6, we have $L\pi' \in \operatorname{Rec} M'$. Together with condition (iii), this implies $L\pi \in \operatorname{Rec} M$ by Theorem 5.2. □

Corollary 5.8. *Let $A \in \operatorname{Rat} M$ and let n be the maximum number of vertices of $\min_{\widetilde{A}}$, $\min_{\overline{A}}$. Then $A \in \operatorname{Rec} M$ is decidable with polynomial complexity with respect to $n + |X|$.*

Proof. It is enough to give polynomial bounds for conditions (i)–(iii) of Theorem 4.4. This is trivial for (i), and a polynomial bound for (iii) follows from Corollary 4.5. The nontrivial inclusion in (ii) remains to be considered.

Indeed, $L(\widetilde{D(\min_{\widetilde{A}})}) \subseteq \widetilde{A}$ is equivalent to saying that

$$L(\widetilde{D(\min_{\widetilde{A}})}) \cap (X^* \setminus \widetilde{A}) = \emptyset.$$

On the one hand, $D(\min_{\widetilde{A}})$ has still at most n vertices, and so $L(\widetilde{D(\min_{\widetilde{A}})})$ has at most $n(|X| + 1)$ vertices [2].

On the other hand, $\min_{\widetilde{A}}$ can be easily adapted to recognize $X^* \setminus \widetilde{A}$, adding at most one extra vertex, and now we can decide empty intersection using the direct product of these two automata, which can certainly be done at polynomial cost. □

Thus we obtain a much more efficient algorithm for deciding recognizability in comparison with the one arising from Section 3, that involves at least double exponential complexity.

Acknowledgements

The author acknowledges support from F.C.T. through C.M.U.P. and the project POCTI/MAT/37670/2001, with funds from the programs POCTI and POSI, with national and European Community structural funds.

References

[1] S.I. Adyan, Defining relations and algorithmic problems for groups and semigroups, Proc. Steklov Inst. Math. 85 (1966) 152. Translation from Tr. Mat. Inst. Steklov 85, (1966) 123 (in Russian, English).
[2] M. Benois, Descendants of regular language in a class of rewriting systems: Algorithm and complexity of an automata construction, in: Proceedings RTA 87, in: LNCS, vol. 256, 1987, pp. 121–132.
[3] J. Berstel, Transductions and Context-free Languages, Teubner, 1979.
[4] R.V. Book, F. Otto, String-Rewriting Systems, Springer-Verlag, New York, 1993.
[5] L. Chottin, Langages algébriques et systèmes de réécriture rationnels, RAIRO Theoret. Inform. Appl. 16 (1982) 1–20.
[6] J.E. Hopcroft, J.D. Ullman, Introduction to Automata Theory, Languages and Computation, Addison-Wesley, 1979.
[7] J. Sakarovitch, Syntaxe des Langages de Chomsky — Essai sur le Déterminisme, Thèse de Doctorat d'État, Univ. Paris VII, 1979.
[8] G. Sénizergues, The equivalence and inclusion problems for NTS languages, J. Comput. Syst. Sci. 31 (3) (1985) 303–331.
[9] G. Sénizergues, Some decision problems about controlled rewriting systems, Theoret. Comput. Sci. 71 (1990) 281–346.
[10] G. Sénizergues, On the rational subsets of the free group, Acta Inform. 33 (1996) 281–296.
[11] G. Sénizergues, A polynomial algorithm testing partial confluence of basic semi-Thue systems, Theoret. Comput. Sci. 192 (1) (1998) 55–75.
[12] G. Sénizergues, $L(A) = L(B)$? decidability results from complete formal systems, Theoret. Comput. Sci. 251 (1–2) (2001) 1–166.
[13] P.V. Silva, Free group languages: rational versus recognizable, RAIRO Theoret. Informatics Appl. 38 (2004) 49–67.
[14] P.V. Silva, Recognizable subsets of a group: finite extensions and the abelian case, Bull. E.A.T.C.S. 77 (2002) 195–215.
[15] L.G. Valiant, Regularity and related problems for deterministic pushdown automata, J. Assoc. Comput. Mach. 22 (1975) 1–10.