View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

Theoretical Computer Science 66 (1989) 55-63
North-Holland

AN EFFICIENT ALGORITHM TO DECIDE WHETHER A MONOID PRESENTED BY A REGULAR CHURCH-ROSSER THUE SYSTEM IS A GROUP

Zhang Luo XIN

Department of Mathematics, Lanzhou University, Lanzhou, Gansu, People's Rep. China

Communicated by R. Book
Received August 1987
Revised January 1988

Abstract. We give an $O(|A|^2 \times |T|)$ algorithm that on the input of a regular Church-Rosser Thue system T on alphabet A decides whether or not the monoid M_T presented by T is a group, where $|A|$ is the cardinality of A, and $|T|$ is the size of the Thue system T. In addition, a problem is presented that is decidable for regular monadic Church-Rosser Thue systems, but that is undecidable for finite non-monadic Church-Rosser Thue systems.

Introduction

The Church-Rosser property has been shown to be a very powerful tool in providing decidability results for monoids. Many decision problems for monoids, that are undecidable in general, become decidable when they are restricted to presentations involving the Church-Rosser property [2-5, 12, 13, 15, 16]. In addition, Nivat and co-workers studied the Church-Rosser property when they investigated Thue congruences that specify formal languages [6, 14].

It is well known that there is no algorithm to decide whether or not a monoid presented by a Thue system is a group. There are cases where this problem is decidable [1, 3, 4, 11, 16].

In [3], Book gave a polynomial-time algorithm to decide whether or not a monoid presented by a finite monadic Church-Rosser Thue system is a group, but for an infinite monadic Church-Rosser Thue system, the algorithm uses polynomial space; later, by developing the technique of linear sentences [4], Book gave an $O(|A|^5 \times |T|)$ algorithm to decide whether or not the monoid M_T presented by a regular monadic Church-Rosser Thue system T on alphabet A is a group, where $|A|$ is the cardinality of A, and $|T|$ is the size of the Thue system T. Here we give an $O(|A|^2 \times |T|)$ algorithm to decide the problem for regular Church-Rosser Thue systems T on A. (See [7], for a discussion of the role of tractable problems and polynomial-time algorithms.) In addition, we show that, given a finite Church-Rosser Thue system T on A and a letter $a \in A$, it is undecidable whether or not a has a right-inverse in M_T, but this

0304-3975/89/$3.50 © 1989, Elsevier Science Publishers B.V. (North-Holland)

problem becomes decidable when it is restricted to monadic Church-Rosser Thue systems.

1. Preliminaries

It is assumed that the reader is familiar with the basic results in the theories of automata, computability and formal languages as covered in a text such as that of Hopcroft and Ullman [8]. In this section, the notation is established and the basic definitions and properties of Thue systems and congruences are described.

If A is a finite alphabet, then A^* is the free monoid with identity e generated by A. If w is a string, then the *length* of w is denoted by $|w|$: $|e|=0$, $|a|=1$ for $a\in A$, and $|wa|=|w|+1$ for $w\in A^*$, $a\in A$.

For a finite set S of strings, let $|S|=\sum_{w\in S}|w|$.

A *Thue system* T on alphabet A is a subset of $A^*\times A^*$, in which each pair in T is called a *rule*. The *Thue congruence* generated by T is the reflexive transitive closure $\overset{*}{\leftrightarrow}_T$ of the relation $\leftrightarrow_T$ defined as follows: for any $u, v\in A^*$ such that $(u, v)\in T$ or $(v, u)\in T$, and any $x, y\in A^*$, $xuy\leftrightarrow_T xvy$. Two strings w, z are *congruent* (mod T) if $w\overset{*}{\leftrightarrow}_T z$. The congruence class of z (mod T) is $[z]_T=\{w: w\overset{*}{\leftrightarrow}_T z\}$. Whenever possible the subscript T will be omitted.

If T is a Thue system on A, then the congruence classes of T form a monoid M_T under the multiplication $[x].[y]=[xy]$; the identity is $[e]$. This is the *monoid presented* by T [10].

If T is a Thue system, write $x\to y$ provided $x\leftrightarrow y$ and $|x|>|y|$, and write $\overset{*}{\to}$ for the reflexive transitive closure of the relation $\to$. The relation $\to$ is called *reduction*. If $u\overset{*}{\to}v$, we say that u reduces to v, u is an *ancestor* of v, and v is a *descendant* of u(mod T). If u has no descendants except itself, then it is *irreducible*, otherwise it is *reducible* (mod T).

A Thue system T is Church-Rosser if for all $x, y\in A^*$, $x\overset{*}{\leftrightarrow}y$ implies that for some z, $x\overset{*}{\to}z$ and $y\overset{*}{\to}z$. Thus, we can show that in a Church-Rosser Thue system, every congruence class contains exactly one irreducible, which is the shortest string in its congruence class, and every string can effectively be reduced to the irreducible string in its class. In fact, this is essentially why the Church-Rosser systems are very well-behaved.

Given a Thue system T, let

$$\text{domain}(T)=\{u: \exists v\,((u, v)\in T)\};\qquad \text{range}(T)=\{v: \exists u\,((u, v)\in T)\}.$$

A Thue system on A is

(1) *monadic* if

(i) $\text{range}(T)\subseteq A\cup\{e\}$;

(ii) for every u, v such that $(u, v)\in T$, $|u|>|v|$.

(2) *regular* if

(i) $\text{range}(T)$ is finite;

(ii) for every $v\in\text{range}(T)$, $R_v=\{u: (u, v)\in T\}$ is a regular language.

(3) *context-free* if
  (i) range(T) is finite;
  (ii) for every $v \in \text{range}(T)$, $R_v = \{u: (u, v) \in T\}$ is a context-free language.
(4) *reduced* if, for each rule $(u, v) \in T$, u cannot be reduced by any other rule of T, and v is irreducible modulo T.

It is well known that the Church-Rosser property is decidable for regular monadic Thue systems [15], but not for context-free monadic Thue systems [5]. Regular monadic Thue systems and context-free monadic Thue systems are studied respectively in [15] and [5].

Let T be a regular Church-Rosser Thue system on A such that M_T is a group. If T is reduced, by using the pumping lemma for regular languages, we have that T is finite. Thus, non-reduced systems are being considered in this paper.

2. The main results

Let V and A be disjoint finite alphabets and let $S \in V$. Let $P \subseteq V \times A^*(V \cup \{e\})$ be finite, and let $\Rightarrow \subseteq (V \cup A)^* \times (V \cup A)^*$ be the relation defined as follows: if $(Z, y) \in P$, then for all $u, v \in (V \cup A)^*$, $uZv \Rightarrow uyv$. The reflexive transitive closure of $\Rightarrow$ is denoted by $\Rightarrow^*$. The structure $G = (V, A, P, S)$ is a *regular grammar* and the *language* generated by G is $L(G) = \{w \in A^*: S \Rightarrow^* w\}$. A language L is *regular* if and only if there is a regular grammar G such that $L(G) = L$. The *size* of a regular grammar $G = (V, A, P, S)$ is

$$|G| = |V| + |A| + \sum_{(Z,y) \in P} (|Z| + |y|).$$

Assume that a regular Thue system is presented as a list of pairs of the form (G_v, v), where G_v is a regular grammar for R_v. Then the *size* of T is defined as

$$|T| = \sum_{v \in \text{range}(T)} (|G| + |v|).$$

Now the main results can be established.

Theorem 2.1. *There is an* $O(|A|^2 \times |T|)$ *algorithm to decide the following problem: given a regular Church-Rosser Thue system on A, is the monoid* M_T *presented by T a group?*

First, we give a lemma which will be needed in the proof of Theorem 2.1.

Let T be a Thue system on A. We denote

$$s(T) = \{(u, e): (u, e) \in T\},$$

and define a sequence of subsets of A as follows:

$$A_1 = \{a: \exists u \in A^*: (au, e) \in s(T)\};$$
$$A_{i+1} = A_i \cup \{a \in A - A_i: \exists u \in A^*, \exists v \in A_i^*: (au, v) \in T\} \tag{2.1}$$

for each integer $i \geq 1$. Obviously, $A_1 \subseteq A_2 \subseteq \cdots \subseteq A_i \subseteq A_{i+1} \subseteq \cdots \subseteq A$. Since A is finite, there is an integer $k \leq |A|$ such that $A_k = A_{k+j}$ for each integer $j \geq 0$. Furthermore, if $A_{|A|} \neq A$, then there is an integer $k < |A|$ such that $A_k = A_{k+j}$ for each integer $j \geq 0$.

Lemma 2.2. *Let T be a Church-Rosser Thue system on A. Then the monoid M_T presented by T is a group if and only if there is an integer $k \leq |A|$ such that $A_k = A$.*

Proof. ($\Leftarrow$): The monoid M_T is a group if and only if, for each string $u \in A^*$, there exists a string $u' \in A^*$ such that $uu' \overset{*}{\leftrightarrow} e$. Obviously, this is equivalent to saying that for each letter $a \in A$, there exists a string $w \in A^*$ such that $aw \overset{*}{\leftrightarrow} e$, i.e., a has a right-inverse. Let $A_k = A$ for some $k \leq |A|$, and let $a \in A_m - A_{m-1}$, where $m \leq k$. Then a has a right-inverse, because: if $m = 1$, then $(au, e) \in T$ for some $u \in A^*$. If $m > 1$, then $(au, v) \in T$ for some $u \in A^*$, $v \in A^*_{m-1}$. Let $v = b_1 b_2 \ldots b_r$, where $b_j \in A_{m-1}$ for each j. Then by the induction hypothesis, each b_j has a right-inverse, i.e., there exists some u_j such that $b_j u_j \overset{*}{\leftrightarrow} e$ for each j. Take $w = uu_r u_{r-1} \ldots u_1$. Then

$$aw = auu_r u_{r-1} \ldots u_1 \rightarrow vu_r u_{r-1} \ldots u_1 = b_1 \ldots b_{r-1} b_r u_r u_{r-1} \ldots u_1 \overset{*}{\rightarrow} e.$$

Thus M_T is a group.

($\Rightarrow$): Let M_T be a group. Assume that $A_{|A|} \subsetneq A$, i.e., $A_k = A_{k+1} \neq A_{|A|}$ for some $k < |A|$. Let $a \in A - A_k$ such that the inverse a^{-1} is of minimal length. Since T is a Church-Rosser Thue system and M_T is a group, $aa^{-1} \overset{*}{\rightarrow} e$, and since a^{-1} is irreducible, $a^{-1} = ux$ with $(au, v) \in T$, $v \neq e$. Hence, $aa^{-1} = aux \rightarrow vx$. Let $v = ybz$, $y, z \in A^*$, $b \in A$. Then $vx \overset{*}{\leftrightarrow} e$, and since M_T is a group, $bzxy \overset{*}{\leftrightarrow} e$. Thus,

$$|b^{-1}| \leq |zxy| < |vx| \leq |ux| = |a^{-1}|.$$

From the choice of a we conclude that $b \in A_k$. Hence, $v \in A_k^*$ implies that $a \in A_{k+1} \subseteq A_{|A|}$. Contradiction! Thus, $A = A_{|A|}$. □

The Thue system $T = \{(abbaab, e)\}$ studied by Jantzen [9] is not Church-Rosser. For this system, $A_i = \{a\}$ for each $i \geq 1$. However, M_T is a group. This example indicates that the Church-Rosser property is necessary in Lemma 2.2.

Proof of Theorem 2.1. Lemma 2.2 gives us the following algorithm to decide whether or not M_T is a group.

Group Procedure (T):

(1) $i := 1$
(2) $T_1 := s(T)$
(3) $C := \text{alph}(T_1)$ $(= \{a \in A: \exists u \in A^*: (au, e) \in T_1\})$
(4) $B := C$
(5) **while** $i \leq |A|$ **do**
(6) $\quad C := C \cup B$
(7) $\quad$ **if** $C = A$

(8) **then** announce "T has the group-property" and exit
(9) **if** $B=\emptyset$
(10) **then** announce "T has not the group-property" and exit
(11) $i := i+1$
(12) $T_i := T(B)\ (=\{(u, v)\in T: v\in B^*\})$
(13) $B := \mathrm{alph}(T_i)-C$
(14) **endwhile**

Given a regular grammar G and a letter $a\in A$, the question "$L(G)\cap aA^*=\emptyset$" can be decided in $O(|G|)$ by using breadth-first search. Thus the time for executing (3) (or (13)) is $O(|A|\times|T|)$, and the procedure above can be accomplished in $O(|A|^2\times|T|)$ because of the **while**-loop (5). □

The same results as presented in Theorem 2.1 were independently obtained by Narendran and Otto [13].

Theorem 2.1 can be extended in the following ways.

(1) Let G be a context-free grammar, and $a\in A$. Then $L(G)\cup aA^*$ is also context-free, we can obtain a context-free grammar G_a such that $L(G_a)=L(G)\cup aA^*$, and the size of G_a (the definition of the size is similar to that of a regular grammar) is at worst $O(|G|^2)$. The question "$L(G_a)=\emptyset$" can be decided in polynomial time. Thus we can decide whether or not a monoid presented by a context-free Church-Rosser Thue system is a group in polynomial time.

(2) Let T be a Thue system on A. T is called *almost-confluent* if for all $x, y\in A^*$ such that $x\overset{*}{\leftrightarrow}y$, then there exist g, h such that $x\overset{*}{\rightarrow}g$, $y\overset{*}{\rightarrow}h$, and $g\overset{*}{\vdash\!\dashv}h$, where $\overset{*}{\vdash\!\dashv}$ is the reflexive transitive closure of the relation $\vdash\!\dashv$ defined as follows: $x\vdash\!\dashv y$ if and only if $x\leftrightarrow y$ and $|x|=|y|$. If T is almost-confluent, then for each $w\in A^*$, $w\overset{*}{\leftrightarrow}e$ if and only if $w\overset{*}{\rightarrow}e$. Therefore, the condition "Church-Rosser" can be replaced by the condition "almost-confluent" in Theorem 2.1.

(3) If T is a finite Church-Rosser Thue system, the time for executing (3) (or (13)) is $O(|T|)$, and thus the overall time becomes $O(|A|\times|T|)$.

Finally, note that it is not at all clear how this method could be applied to deciding whether or not a finitely generated submonoid is a group.

3. A problem that is decidable for regular monadic Church–Rosser Thue systems but that is undecidable for finite non-monadic Church–Rosser Thue systems

Let T be a Thue system on A. The monoid M_T presented by T is a group if and only if all letters from A have a right-inverse in M_T. Thus, given a regular Church-Rosser Thue system T on A, one can decide whether or not *all* letters from A have a right-inverse in M_T. Then one may formulate the following decision problem.

Right-Inverse

Instance: A Thue system T on A, and a letter $a\in A$.

Question: Does a have a right-inverse in M_T?

In this section, we show that this problem is decidable for regular monadic Church-Rosser Thue systems, but that it is undecidable for finite non-monadic Church-Rosser Thue systems.

By using the technique of linear sentences developed by Book, we can prove that the problem Right-Inverse is decidable for monadic Church-Rosser Thue systems. In fact, a letter $a \in A$ has a right-inverse in M_T if and only if the following linear sentence is true under the interpretation induced by T: $\exists u \in A^*$: $au \overset{*}{\leftrightarrow}_T e$. But we give here another proof more suited to our purposes.

Let T be a monadic Thue system on A. Formula (2.1) can be rewritten as follows:

$$A_1 = \{a: \exists u \in A^*: (au, e) \in s(T)\};$$

$$A_{i+1} = A_i \cup \{a \in A - A_i: \exists u \in A^*: (au, b) \in T \text{ for some } b \in A_i\}$$

for each integer $i \geqslant 1$.

Lemma 3.1. *Let T be a monadic Church-Rosser Thue system on A and $a \in A$. Then, a has a right-inverse if and only if $a \in A_{|A|}$.*

Proof. ($\Leftarrow$): Let $a \in A_{|A|} \subseteq A$. Then there exists an integer $m \leqslant |A|$ such that $a \in A_m - A_{m-1}$, and we have $a_1 = a, a_2, \ldots, a_{m-1}, u_1 u_2 \ldots, u_{m-1}$, where $a_i \in A$ and $u_i \in A^*$ for each $i = 1, 2, \ldots, m-1$, such that $(a_i u_i, a_{i+1}) \in T$ for $i = 1, 2, \ldots, m-2$, and $(a_{m-1} u_{m-1}, e) \in s(T)$. Letting $u = u_1 u_2 \ldots u_{m-1}$, we have

$$au = au_1 u_2 \ldots u_{m-1} \rightarrow a_2 u_2 \ldots u_{m-1} \overset{*}{\rightarrow} a_{m-1} u_{m-1} \rightarrow e$$

i.e., $au \overset{*}{\rightarrow} e$. Therefore, a has a right-inverse in M_T.

($\Rightarrow$): Let T be a monadic Church-Rosser Thue system on alphabet A. Then we can derive the following claim:

Claim. *Let $w = au \in A^*$, where $a \in A$ and $u \in A^*$, such that*

$$w \rightarrow w_1 \rightarrow w_2 \rightarrow \cdots \rightarrow w_j = e,$$

then $a \in A_j$.

Proof. By induction over j. $j = 1$: $w = au \rightarrow w_1 = e$, then $a \in A_1$ and the conclusion holds.

If the conclusion holds for $j \leqslant m$, suppose now that

$$w = au \rightarrow w_1 \rightarrow w_2 \rightarrow \cdots \rightarrow w_{m+1} = e.$$

If $a \in A_m$, then $a \in A_{m+1}$. Otherwise, assuming without loss of generality that u is irreducible, au can be factorized as avs, where for some $c(av, c) \in T$ and $w_1 = cs$. Since $a \notin A_m$, $c \neq e$. By induction hypothesis, $c \in A_m$; therefore $a \in A_{m+1}$.

Therefore, the conclusion of the claim holds. □

If a has a right-inverse, then $au \overset{*}{\leftrightarrow} e$ for some $u \in A^*$, and since T is Church-Rosser, $au \overset{*}{\rightarrow} e$. Therefore, by the claim above, there is a k such that $a \in A_k$, so $a \in A_{|A|}$. □

By using Lemma 3.1, we can prove the following theorem.

Theorem 3.2. *There is an* $O(|A|^2 \times |T|)$ *algorithm to decide the problem Right-Inverse for regular monadic Church-Rosser Thue systems.*

The similar conclusion in Lemma 3.1 is not true for non-monadic Church-Rosser Thue systems. For example, let $T = \{(abc, e), (fgh, ab)\}$. Then T is Church-Rosser and $A_i = \{a\}$ for each $i \geq 1$. But f has a right-inverse in M_T. Of course, this does not imply that the problem Right-Inverse is undecidable for finite non-monadic Church-Rosser Thue systems, since there might be other ways to obtain a decision algorithm for the problem. However, we will see that the problem is undecidable for finite non-monadic Church-Rosser Thue systems.

First, we construct a finite Church-Rosser Thue system to simulate a Turing machine. This observation was first made by Jantzen and Monien (communicated by Book).

Let $M = (\Sigma, Q, q_0, \delta)$ be a single tape Turing machine. Here $Q = \{q_0, q_1, \ldots, q_n\}$, $q_0 \in Q$ is the initial state, and

$$\delta\colon Q \times (\Sigma \cup \{b\}) \to Q \times (\Sigma \cup \{b\}) \times \{\mathrm{L}, \mathrm{R}\}$$

is the transition function of M, where b denotes the blank symbol, and L and R denote the moves of M's head. Note that we assume that M moves its head in every step.

Furthermore, we assume that M cannot print the blank symbol, and whenever it halts, it halts on the leftmost square it has ever visited in a unique state q_n, and no transition is possible from within state q_n. Then, we have the following results (similar results can be found in [12]).

Theorem 3.3 (F. Otto [17]). *There exists a finite Church-Rosser Thue system* $T(M)$ *on* $\Gamma \supseteq \Sigma \cup \{\$, \not\in\}$ *with the following properties*:

(a) *Let* $w \in S = \{\$\}(\Sigma_b \cup D)^* \cdot (Q_p \cup Q_s) \cdot (\Sigma_b \cup D)^*\{\not\in\}$, *where* $\Sigma_b = \Sigma \cup \{b\}$, $D \subseteq \Gamma$ *such that* $D \cap (Q_p \cup Q_s) = D \cap \Sigma_b = \emptyset$, *and both* $Q_p = \{p_0, p_1, p_2, \ldots, p_n\}$ *and* $Q_s = \{s_0, s_1, s_2, \ldots, s_n\}$ *are disjoint copies of* Q. *If* $w \xrightarrow{*}_{T(M)} z$, *then* $z \in S$;

(b) M *halts on input* x *if and only if*

$$\exists w \in \$p_n\Gamma^*\not\in\colon \quad w \xrightarrow{*}_{T(M)} \$s_0x\not\in.$$

(c) (1) *If* $(\$u, v) \in T(M)$, *then* $v = \$p_i$, *and* $u = d_1as_j$, *or* $u = p_kcd_2$ *for some* $i, j, k \leq n$, $a, c \in \Sigma_b$ *and* $d_1, d_2 \in D$.

(2) *If* $(u, v\not\in) \in T(M)$, *then* $v = s_i$, *and* $u = d_1as_j\not\in$ *or* $u = p_kcd_2\not\in$ *for some* $i, j, k \leq n$, $a, c \in \Sigma_b$, *and* $d_1, d_2 \in D$.

(d) *Every left-hand side of a rule of* $T(M)$ *does not begin in* $\not\in$ *and does not end in* \$.

(e) $\mathrm{range}(T(M)) \subseteq \Gamma \cup \Gamma^2$.

Continuing the notation of Theorem 3.3, given an input string x, let $A = \Gamma \cup \{\bar{a}, \bar{b}, \bar{c}\}$, and

$$T_x = T(M) \cup \{(\bar{a}\bar{b}\bar{c}, \$p_n), (\$s_0 x \not{c}, e)\}.$$

Since no left-hand side of a rule of $T(M)$ begins in $\not{c}$ or ends in \$, new rules produce no additional critical pairs. Thus T_x is also Church-Rosser.

Lemma 3.4. *Given T_x as above, then the letter $\bar{a}$ has a right-inverse in M_{T_x} if and only if Z halts on input x.*

Proof ($\Leftarrow$): *If Z* halts on input x, then, by the property (b) in Theorem 3.3, there exists $y \in \Gamma^*$ such that $\$p_n y \not{c} \xrightarrow{*} \$s_0 x \not{c}$. Letting $w = \bar{b}\bar{c}y\not{c}$. Then,

$$\bar{a}w = \bar{a}\bar{b}\bar{c}y\not{c} \rightarrow_{T_x} \$p_n y \not{c} \xrightarrow{*}_{T_x} \$s_0 x \not{c} \rightarrow_{T_x} e.$$

Hence, $\bar{a}$ has a right-inverse in M_{T_x}.

($\Rightarrow$): Let $\bar{a}$ have a right-inverse in M_{T_x}. Assume that a^{-1} is the right-inverse of minimal length. Since T is Church-Rosser,

$$\bar{a}a^{-1} \rightarrow_{T_x} w_1 \rightarrow_{T_x} w_2 \rightarrow_{T_x} \cdots \rightarrow_{T_x} w_k \rightarrow_{T_x} e$$

for some $w_i \in A^*$ for each $i = 1, 2, \ldots, k$. Since $\text{range}(T(M)) \subseteq \Gamma \cup \Gamma^2$, $w_k \rightarrow_{T_x} e$ implies $w_k = \$s_0 x \not{c}$. On the other hand, $\bar{a}a^{-1} \rightarrow_{T_x} w_1$ implies that $a^{-1} = \bar{b}\bar{c}v$, and $w_1 = \$p_n v$ for some $v \in A^*$. Now we prove $w_1 = \$p_n v \xrightarrow{*}_{T(M)} w_k = \$s_0 x \not{c}$.

Since $\bar{a}$ (respectively $\bar{b}$, and $\bar{c}$) cannot be introduced, if $\bar{a}$ (respectively $\bar{b}$, and $\bar{c}$) occurs in w_i for some $i \geq 1$, then it must occur in w_1. Because no occurrence of $\bar{a}$ (respectively $\bar{b}$, and $\bar{c}$) is in w_k, then $v = v_1 \bar{a}\bar{b}\bar{c}v_2$ for some $v_1, v_2 \in A^*$. This is impossible, since v is irreducible. Hence, $\bar{a}$ (respectively $\bar{b}$, and $\bar{c}$) does not occur in w_i for each $i = 1, 2, \ldots, k$, and $(\bar{a}\bar{b}\bar{c}, \$p_n)$ cannot be used in $w_1 \xrightarrow{*}_{T_x} w_k$.

An occurrence of the symbol \$ can be introduced only by $(\bar{a}\bar{b}\bar{c}, \$p_n)$. Since the rule $(\bar{a}\bar{b}\bar{c}, \$p_n)$ is not used in $w_1 \xrightarrow{*}_{T_x} w_k$ the rule $(\$s_0 x \not{c}, e)$ is not used in $w_1 \xrightarrow{*}_{T_x} w_k$. Otherwise, since a^{-1} is irreducible, by using the property (c) in Theorem 3.3, $v = z'z$, $w_i = \$s_0 x \not{c} z$ for some z', $z \in A^*$ such that $\$p_n z' \xrightarrow{*}_{T(M)} \$s_0 x \not{c}$, and $|z| > 0$. Then, $\bar{a}$ has a right-inverse $\bar{b}\bar{c}z'$ of length less than $a^{-1} = \bar{b}\bar{c}z'z$. Contradiction! Therefore, $w_1 \xrightarrow{*}_{T(M)} w_k = \$s_0 x \not{c}$.

According to the construction of T_x, $w_1 \in \Gamma^*$, and thus M halts on input x. □

Now, we can establish the following theorem.

Theorem 3.5. *The problem Right-Inverse is undecidable for finite non-monadic Church-Rosser Thue systems.*

Proof. Let $M = (\Sigma, Q, q_0, \delta)$ be the Turing machine whose halting problem is undecidable, and suppose that, whenever Z halts, it halts on the leftmost square it has ever visited, in the unique state q_n, and no transition is ever possible within state

q_n. Furthermore, we assume that Z cannot print the blank symbol. Given an input string x, from above discussion, we can effectively construct a finite non-monadic Church–Rosser Thue system T_x on an alphabet $A \supset \{\bar{a}\} \cup \Sigma$ such that $\bar{a}$ has a right-inverse in M_{T_x} if and only if M halts on input x. Thus Right-Inverse is undecidable for non-monadic Church–Rosser Thue systems. □

Let w^R denote the reversal of the word, i.e., $e^R = e$, and $(wa)^R = aw^R$ for all $w \in A^*$ and $a \in A$. Now let

$$T_x^R = \{(u, v): (u^R, v^R) \in T_x\},$$

and M^R be the monoid presented by R_x^R. Then T_x^R is Church–Rosser, because T_x is, and for T_x^R, a lemma corresponding to Lemma 3.4 holds. Hence, we have the following result: given a finite non-monadic Church–Rosser Thue system T on A, and a letter $a \in A$, it is undecidable whether or not a has a left-inverse in M_T.

Acknowledgment

The author is grateful to Professor Book and the referees for helpful comments and suggestions for improving this paper.

References

[1] S. Adjan, Defining relations and algorithmic problems for groups and semigroups, *Proc. Steklov Inst. Math.* **85** (1966).
[2] R. Book, Confluent and other types of Thue systems, *J. ACM* **29** (1982) 171–182.
[3] R. Book, When is a monoid a group? The Church–Rosser case is tractable, *Theoret. Comput. Sci.* **18** (1982) 325–331.
[4] R. Book, Decidable sentences of Church–Rosser congruences, *Theoret. Comput. Sci.* **24** (1983) 301–312.
[5] R. Book, M. Jantzen and C. Wrathall, Monadic Thue systems, *Theoret. Comput. Sci.* **19** (1982) 231–251.
[6] Y. Cochet and M. Nivat, Une généralization des ensembles de Dyck, *Israel J. Math.* **9** (1971) 389–395.
[7] M. Garey and D. Johnson, *Computers and Intractability* (Freeman, San Francisco, CA, 1979).
[8] J. Hopcroft and J. Ullman, *Introduction to Automata Theory, Languages, and Computation* (Addition-Wesley, Reading, MA, 1979).
[9] M. Jantzen, On a special monoid with a single defing relation, *Theoret. Comput. Sci.* **16** (1981) 61–73.
[10] G. Lallement, *Semigroups and Combinatorial Applications* (Wiley-Interscience, New York, 1979).
[11] G. Lallement, On monoids presented by a single relation, *J. Algebra* **32** (1974) 370–388.
[12] P. Narendran, C. Ó' Dúnlaing and H. Rolletschek, Complexity of certain decision problems about congruential languages, *J. Comput. System Sci.* **30** (1985) 343–357.
[13] P. Narendran and F. Otto, Elements of finite order for finite Church–Rosser Thue systems, *Acta Inform.* **25** (1988) 573–591.
[14] M. Nivat, On some families of languages related to the Dyck Languages, in: *Proc. 2nd ACM Symp. on Theory of Computing* (1970) 221–225.
[15] C. Ó'Dúnlaing, Infinite regular Thue systems, *Theoret. Comput. Sci.* **25** (1983) 171–192.
[16] F. Otto, On deciding whether a monoid is a free monoid or is a group, *Acta Inform.* **23** (1986) 99–110.
[17] F. Otto, Some undecidability results for non-monadic Church–Rosser Thue systems, *Theoret. Comput. Sci.* **33** (1984) 261–278.