ELEMENTS OF FINITE ORDER
FOR FINITE MONADIC CHURCH–ROSSER THUE SYSTEMS

BY

FRIEDRICH OTTO

ABSTRACT. A Thue system T over Σ is said to allow nontrivial elements of finite order, if there exist a word $u \in \Sigma^*$ and integers $n \geq 0$ and $k \geq 1$ such that $u \leftrightarrow_T^* \lambda$ and $u^{n+k} \leftrightarrow_T^* u^n$. Here the following decision problem is shown to be decidable:

Instance. A finite, monadic, Church–Rosser Thue system T over Σ.

Question. Does T allow nontrivial elements of finite order?

By a result of Muller and Schupp this implies in particular that given a finite monadic Church–Rosser Thue system T it is decidable whether the monoid presented by T is a free group or not.

Introduction. Thue systems are string rewriting systems often studied in computability theory, combinatorial (semi-) group theory, and formal language theory. They are used to present monoids and groups [13, 15], and to specify languages as unions of congruence classes, leading to the class of "congruential languages" [3, 9, 19].

Thue systems that satisfy the Church–Rosser property [3, 4, 9] are of special interest, since a finite Church–Rosser Thue system defines a unique normal form for each of its congruence classes, and any word can be reduced in linear time to the normal form of its class [4]. If in addition to being finite and Church–Rosser, a Thue system T is monadic, then many decision problems for T are decidable, e.g., the power problem, the generalized word problem for regular sets, the independent set problem for finite sets [6], and the problem of deciding of whether the monoid presented by T is a group [5]. By using the results of [7, 8] it can be shown easily that also the following problem is decidable for a finite, monadic, Church–Rosser Thue system T over Σ:

Instance. A word $w \in \Sigma^*$.

Question. Is w a nontrivial element of finite order for T?

Here we want to consider the following generalization of the problem stated above:

(∗) *Instance.* A finite Thue system T over Σ.

Question. Does there exist a nontrivial element of finite order for T?

This problem is undecidable in general, since the property of not having nontrivial elements of finite order is a Markov property [16], (see, e.g., [17]). On the other hand, Lallement has given a syntactic characterization for those one-rule Thue systems that

have nontrivial elements of finite order [12]. Here we will prove that problem (∗) is decidable when it is restricted to finite Thue systems that are monadic and Church–Rosser.

After giving the basic definitions and notation, we first deal with the problem of deciding whether or not a given Thue system has a nontrivial idempotent. Since idempotents are specific elements of finite order, this is a restriction of problem (∗). In §2 this restricted problem is solved for finite, special, Church–Rosser Thue systems, and in §3 this solution is extended to finite, monadic, Church–Rosser Thue systems. Then this result is used in §4 to establish our main result, which states that it is decidable whether or not there exist nontrivial elements of finite order for a given finite, monadic, Church–Rosser Thue system. Finally, we give an application of the main result to the problem of deciding whether or not the monoid presented by a given finite, monadic, Church–Rosser Thue system is a free group.

1. Preliminaries. Let Σ be a finite alphabet, and let Σ^* be the set of all words over Σ including the empty word λ, i.e., Σ^* is the free monoid generated by Σ under the operation of concatenation with the empty word λ as identity. For $w \in \Sigma^*$, the *length* of w is denoted by $|w|$: $|\lambda| = 0$, and $|wa| = |w| + 1$ for all $w \in \Sigma^*$ and $a \in \Sigma$. The *concatenation* of words u and v is simply written as uv, and numerical superscripts are used to abbreviate words, i.e., for all $w \in \Sigma^*$, $w^0 = \lambda$, and $w^{n+1} = ww^n$ for all $n \geq 0$.

A *Thue system* T over Σ is a subset of $\Sigma^* \times \Sigma^*$. The members of T are called (*rewriting*) rules. For a Thue system T over Σ, domain(T) = $\{l | \exists r \in \Sigma^*: (l, r) \in T\}$, and range($T$) = $\{r | \exists l \in \Sigma^*: (l, r) \in T\}$. A Thue system T is called *special*, if domain(T) $\subseteq \Sigma^* - \{\lambda\}$ ($= \Sigma^+$), and range(T) = $\{\lambda\}$, and it is called *monadic* if all the rules of T are length-reducing, and range(T) $\subseteq \Sigma \cup \{\lambda\}$.

For a Thue system T over Σ, the relation $\leftrightarrow_T$ is defined as follows: $\forall u, v \in \Sigma^*$: $u \leftrightarrow_T v$ if and only if $\exists x, y \in \Sigma^*$, $(l, r) \in T$: $(u = xly$ and $v = xry)$ or $(u = xry$ and $v = xly)$. Then the reflexive and transitive closure $\leftrightarrow_T^*$ of $\leftrightarrow_T$ is a congruence on Σ^*, the *Thue congruence* generated by T. If $u \leftrightarrow_T^* v$, one says that u and v are *congruent* (*modulo* T). The *congruence class* $[u]_T$ of u is the set $\{v \in \Sigma^* | v \leftrightarrow_T^* u\}$.

It is well known that the set of congruence classes $\{[u]_T | u \in \Sigma^*\}$ forms a monoid under the operation $[u]_T \circ [v]_T = [uv]_T$ with identity $[\lambda]_T$. This monoid is denoted as $\Sigma^*/\leftrightarrow_T^*$, and the ordered pair $(\Sigma; T)$ is called a *presentation* of this monoid.

Let T be a Thue system over Σ. A word $w \in \Sigma^*$ is called an *element of finite order for T* if there exist integers $n \geq 0$ and $k \geq 1$ such that $w^{n+k} \leftrightarrow_T^* w^n$. If in addition $w \leftrightarrow_T^* \lambda$ does not hold, i.e., $w \not\leftrightarrow_T^* \lambda$, then w is a *nontrivial element of finite order for T*.

In this paper we are concerned with the problem of deciding whether or not there exist nontrivial elements of finite order for a given Thue system T over Σ. More formally this problem is stated as follows:

Instance. A finite Thue system T over Σ.

Question. Does there exist a nontrivial element of finite order for T?

In general, this problem is undecidable, since the property of not having nontrivial elements of finite order is a Markov property [16], (see, e.g., [17]). However, we want

to restrict our attention to finite, monadic, Church–Rosser Thue systems. Here a Thue system T over Σ is called *Church–Rosser* if, for every choice of x and y, $x \leftrightarrow^*_T y$ implies that, for some $z \in \Sigma^*$, $x \to^*_T z$ and $y \to^*_T z$, where $\to^*_T$ denotes the reflexive and transitive closure of the relation $\to_T$ defined as follows: $\forall u, v \in \Sigma^*$: $u \to_T v$ if and only if $u \leftrightarrow_T v$ and $|u| > |v|$. If $x \to^*_T y$, then x is an *ancestor* of y and y is a *descendant* of x (modulo T). A word w is *irreducible* (modulo T) if there is no y such that $w \to_T y$; otherwise, w is *reducible* (modulo T). With IRR(T) we denote the set of all irreducible words.

If T is a finite Thue system over Σ, then the set IRR(T) is a regular set. If T is finite and monadic, then for each regular set $R \subseteq \Sigma^*$, the set $\Delta^*_T(R) = \{ y \in \Sigma^* | \exists w \in R: w \to^*_T y \}$ of descendants of R modulo T is itself a regular set [7], and if, in addition, T is Church–Rosser, then for each regular set $R \subseteq \Sigma^*$, the set $[R]_T = \{ y \in \Sigma^* | \exists w \in R: w \leftrightarrow^*_T y \}$ is a deterministic context-free language [7]. In particular, for a finite, monadic, Church–Rosser Thue system, the word problem is decidable in linear time [4].

2. Idempotents for special Church–Rosser Thue systems. Let T be a Thue system over Σ. A word $u \in \Sigma^*$ is called an *idempotent for T* if it satisfies $u^2 \leftrightarrow^*_T u$. If, in addition, $u \leftrightarrow^*_T \lambda$, then u is a *nontrivial idempotent for T*.

Obviously, a nontrivial idempotent is a nontrivial element of finite order. Thus, if we can show that a given Thue system T has a nontrivial idempotent, then we know that T allows nontrivial elements of finite order.

In this section we are dealing with the problem of deciding for a given finite special Church–Rosser Thue system T over Σ, whether or not there exists a nontrivial idempotent $u \in \Sigma^*$ for T.

Let T be a Thue system over Σ. Two words $u, v \in \Sigma^*$ are *cyclically equal modulo T* ($u \approx_T v$), if there exist words $x, y \in \Sigma^*$ such that $xy \leftrightarrow^*_T u$ and $yx \leftrightarrow^*_T v$ [20].

Now we can characterize idempotents for a given special Church–Rosser Thue system as follows:

LEMMA 2.1. *Let T be a special Church–Rosser Thue system over Σ, and let $u \in \Sigma^*$. Then the following three statements are equivalent*:
(i) *the word u is an idempotent for T*;
(ii) $u \approx_T \lambda$;
(iii) *there are words $x, y \in \Sigma^*$ such that $u = xy$ and $yx \to^*_T \lambda$.*

PROOF. (i) $\Rightarrow$ (iii): If u is an idempotent for T, then $u^2 \leftrightarrow^*_T u$. Since T is Church–Rosser, there is a unique irreducible descendant $u_1 \in \Sigma^*$ of u modulo T. Hence, we have $u_1^2 \leftrightarrow^*_T u^2 \leftrightarrow^*_T u \leftrightarrow^*_T u_1$ implying that $u_1^2 \to^*_T u_1$. Since T is special, this shows that $u_1 = x_1 y_1$ for some words $x_1, y_1 \in \Sigma^*$ with $y_1 x_1 \to^*_T \lambda$. Now $u \to^*_T u_1 = x_1 y_1$ implies that $u = xy$ for some words $x, y \in \Sigma^*$ with $x \to^*_T x_1$ and $y \to^*_T y_1$. Hence, $u = xy$ with $yx \to^*_T y_1 x_1 \to^*_T \lambda$.

(iii) $\Rightarrow$ (ii): This is obvious.

(ii) $\Rightarrow$ (i): If $u \approx_T \lambda$, then there exist words $x, y \in \Sigma^*$ such that $u \leftrightarrow^*_T xy$ and $yx \leftrightarrow^*_T \lambda$. Hence, $u^2 \leftrightarrow^*_T xyxy \leftrightarrow^*_T xy \leftrightarrow^*_T u$, i.e., u is an idempotent for T. □

So for a special Church–Rosser Thue system T over Σ, a word $u \in \Sigma^*$ is an idempotent if and only if it can be factored as $u = xy$ with $yx \to_T^* \lambda$. Thus, the Thue system T has a nontrivial idempotent if and only if there exists a nonempty word $u \in \mathrm{IRR}(T)$ of the form $u = xy$ with $yx \to_T^* \lambda$.

Define an operation CYCLE on the set $\mathscr{P}(\Sigma^*)$ of languages on Σ as follows:

$$\mathrm{CYCLE}(L) = \{\, yx \mid xy \in L \,\},$$

i.e., $\mathrm{CYCLE}(L)$ is the language containing all the cyclic permutations of words of L. With the aid of this operation we can express the existence of nontrivial idempotents for a special Church–Rosser Thue system T over Σ as follows: T has a nontrivial idempotent if and only if $\lambda \in \Delta_T^*(\mathrm{CYCLE}(\mathrm{IRR}(T) - \{\lambda\}))$.

Given a finite Thue system T over Σ, we can effectively construct a finite state acceptor $A_1(T)$ for the regular set $\mathrm{IRR}(T) - \{\lambda\}$ [4]. From $A_1(T)$ we get a finite state acceptor $A_2(T)$ for $\mathrm{CYCLE}(\mathrm{IRR}(T) - \{\lambda\})$ (cf. [11]), from which we can construct a finite state acceptor $A_3(T)$ for $\Delta_T^*(\mathrm{CYCLE}(\mathrm{IRR}(T) - \{\lambda\}))$ [8], provided that the Thue system T is monadic. Thus, a finite special Church–Rosser Thue system T has a nontrivial idempotent if and only if the finite state acceptor $A_3(T)$ accepts on input the empty word λ, which can be determined very easily. This proves our first result.

THEOREM 2.2. *The following problem is decidable*:
Instance. A finite, special, Church–Rosser Thue system T over Σ.
Question. Does there exist a nontrivial idempotent for T?

Since, in general, for a finite Thue system T over Σ, a finite state acceptor for the set $\mathrm{IRR}(T) - \{\lambda\}$ is of size $O(2^{|T|})$, where $|T| = \sum_{(l,r)\in T}|l|$, the algorithm presented above runs in exponential time only.

3. Idempotents for monadic Church–Rosser Thue systems. In this section we want to carry over the result of the previous section to monadic Church–Rosser Thue systems. However, as it will turn out, in this case the characterization of idempotents is somewhat more complicated than in the case of special Church–Rosser Thue systems.

LEMMA 3.1. *Let T be a monadic Church–Rosser Thue system over Σ, and let $u \in \Sigma^*$ be a nonempty irreducible word. Then the following are equivalent*:
   (i) *u is an idempotent for T*;
   (ii) (a) $\exists x, y \in \Sigma^*$: $u = xy$ *and* $yx \to_T^* \lambda$, *or* (b) $\exists x, y \in \Sigma^*$, $a \in \Sigma$: $u = xay$, $ayx \nrightarrow_T^* \lambda$, *and* $ayxa \to_T^* a$.

PROOF. If $u = xy$ with $yx \to_T^* \lambda$, then

$$u^2 = x\lfloor yx \rfloor y \to_T^* xy = u,$$

i.e., u is an idempotent. If $u = xay$ with $ayx \nrightarrow_T^* \lambda$ and $ayxa \to_T^* a$, then

$$u^2 = x\lfloor ayxa \rfloor y \to_T^* xay = u,$$

i.e., u is again an idempotent.

On the other hand, if u is an idempotent, then $u^2 \leftrightarrow_T^* u$ implying that $u^2 \to_T^* u$ according to the choice of u. Since T is monadic, there are words $x, x', y, y' \in \Sigma^*$ and some $a \in \Sigma \cup \{\lambda\}$ such that $u = xx' = y'y = xay$ with $x'y' \to_T^* a$. Hence, $x' = ay$ and $y' = xa$.

If $a = \lambda$, then we have $u = xy$ with $yx = x'y' \to_T^* \lambda$, i.e., (ii)(a) is satisfied. If $a \in \Sigma$, then $u = xay$ with $ayxa = x'y' \to_T^* a$. If $ayx \not\to_T^* \lambda$, then (ii)(b) is satisfied; otherwise, $u = x(ay)$ with $(ay)x \to_T^* \lambda$, i.e., (ii)(a) is satisfied. $\square$

For $a \in \Sigma$, let $\mathrm{INT}_T(a) = \{w \in \mathrm{IRR}(T) \mid awa \to_T^* a\}$, and let $|\mathrm{INT}_T(a)|$ denote the cardinality of this set.

LEMMA 3.2. *Let T be a monadic Church–Rosser Thue system over Σ, and let $a \in \Sigma$. If $|\mathrm{INT}_T(a)| \geq 2$, then T has a nontrivial idempotent.*

PROOF. Let $a \in \Sigma$ with $|\mathrm{INT}_T(a)| \geq 2$, and let $w_1, w_2 \in \mathrm{INT}_T(a)$ with $w_1 \neq w_2$. Then for $i = 1, 2$, we have $aw_i a \to_T^* a$, and hence,

$$\underline{aw_i a} w_i \to_T^* aw_i \quad \text{and} \quad w_i \underline{aw_i a} \to_T^* w_i a,$$

i.e., aw_i and $w_i a$ are idempotents for T. If $aw_i \not\to_T^* \lambda$, then aw_i is a nontrivial idempotent for T; if $w_i a \not\to_T^* \lambda$, then $w_i a$ is a nontrivial idempotent for T. So assume that $aw_i \to_T^* \lambda \leftarrow_T^* w_i a$ for $i = 1, 2$. Then $w_1 \leftarrow_T^* w_1 aw_2 \to_T^* w_2$ implying $w_1 = w_2$ since w_1 and w_2 are irreducible. This contradicts the choice of w_1 and w_2. $\square$

Now we can characterize the existence of nontrivial idempotents for a monadic Church–Rosser Thue system as follows:

THEOREM 3.3. *Let T be a monadic Church–Rosser Thue system over Σ. There exists a nontrivial idempotent for T if and only if one of the following three conditions is satisfied*:
  (i) $\exists u \in \mathrm{IRR}(T) - \{\lambda\} \exists x, y \in \Sigma^*$: $u = xy$ and $yx \to_T^* \lambda$, or
  (ii) $\exists a \in \Sigma$: $|\mathrm{INT}_T(a)| \geq 2$, or
  (iii) $\exists a \in \Sigma \exists w \in \mathrm{IRR}(T)$: $\mathrm{INT}_T(a) = \{w\}$ and $aw \not\to_T^* \lambda$.

PROOF. If there exists a $u \in \mathrm{IRR}(T) - \{\lambda\}$ satisfying (i), then this word u is a nontrivial idempotent for T by Lemma 3.1. By Lemma 3.2 condition (ii) implies that there exists a nontrivial idempotent for T. Finally, if $\mathrm{INT}_T(a) = \{w\}$ with $aw \not\to_T^* \lambda$ for some $a \in \Sigma$, then $u = aw$ is a nontrivial idempotent for T.

So assume conversely, that there exists a nontrivial idempotent $u \in \mathrm{IRR}(T) - \{\lambda\}$. Then according to Lemma 3.1, u satisfies condition (i) or there are $x, y \in \Sigma^*$ and some $a \in \Sigma$ such that $u = xay$, $ayx \not\to_T^* \lambda$, and $ayxa \to_T^* a$. Take $w \in \Sigma^*$ to be the irreducible descendant of yx modulo T. Then $aw \not\to_T^* \lambda$, and $awa \to_T^* a$ implying that $w \in \mathrm{INT}_T(a)$. Thus, either condition (ii) is satisfied with a, or condition (iii) is satisfied with a and w. $\square$

Thus, in order to determine whether there exists a nontrivial idempotent for T it is sufficient to check conditions (i)–(iii) of Theorem 3.3. From the proof of Theorem 2.2 given in the previous section, we immediately derive the following.

LEMMA 3.4. *The following problem is decidable*:

Instance. A finite, monadic, Church–Rosser Thue system T over Σ.

Question. Does there exist a word $u \in \mathrm{IRR}(T) - \{\lambda\}$ that can be factored as $u = xy$ with $yx \to_T^* \lambda$?

Lemma 3.4 shows that condition (i) of Theorem 3.3 is decidable.

LEMMA 3.5. *Let T be a finite, monadic, Church–Rosser Thue system over Σ. Then for each $a \in \Sigma$, one can effectively construct a deterministic pushdown automaton M_a that recognizes $\mathrm{INT}_T(a)$. In particular, $\mathrm{INT}_T(a)$ is a deterministic context-free language for each $a \in \Sigma$.*

PROOF. Given a finite, monadic, Church–Rosser Thue system T over Σ and a letter $a \in \Sigma$, one can effectively construct a deterministic pushdown automaton (dpda) M_1 recognizing $[a]_T$ and a finite state acceptor M_2 recognizing $a \cdot \mathrm{IRR}(T) \cdot a$ [4]. From M_1 and M_2 we get a dpda M_3 that recognizes the set $[a]_T \cap a \cdot \mathrm{IRR}(T) \cdot a = \{awa | w \in \mathrm{IRR}(T) \text{ with } awa \leftrightarrow_T^* a\}$. Since T is Church–Rosser, we have $awa \leftrightarrow_T^* a$ if and only if $awa \to_T^* a$. Thus, $[a]_T \cap a \cdot \mathrm{IRR}(T) \cdot a = \{awa | w \in \mathrm{IRR}(T) \text{ with } awa \to_T^* a\} = a \cdot \mathrm{INT}_T(a) \cdot a$. By using well-known techniques for dealing with dpda's (cf. e.g. [10]) a dpda M_4 recognizing the set $\mathrm{INT}_T(a)$ can effectively be constructed from M_3. □

Given a dpda M we can determine the cardinality of the set L recognized by M, and if L is finite, we can compute a list containing all the elements of L. Hence, conditions (ii) and (iii) of Theorem 3.3 are also decidable. We can summerize the results derived in this section as follows:

THEOREM 3.6. *The following problem is decidable*:

Instance. A finite, monadic, Church–Rosser Thue system T over Σ.

Question. Does there exist a nontrivial idempotent for T?

4. Elements of finite order. Let T be a finite, monadic, Church–Rosser Thue system over Σ. If there exists a nontrivial idempotent for T, then this idempotent is a nontrivial element of finite order for T. However, there may exist nontrivial elements of finite order for T, although there is no nontrivial idempotent for T. For example, this situation occurs when the monoid $\Sigma^*/\leftrightarrow_T^*$ is a finite group. Hence, the result given by Theorem 3.6 is not sufficient for our purposes. Fortunately, we can establish a bound for the length of the shortest nontrivial element of finite order for T in case T has no nontrivial idempotents.

LEMMA 4.1. *Let T be a finite, monadic, Church–Rosser Thue system over Σ, and let $\mu = \max\{|l| \, | \, l \in \mathrm{domain}(T)\}$. If there does not exist a nontrivial idempotent for T, then the following are equivalent*:

(i) *there is a nontrivial element of finite order for T*;

(ii) *there is a word $w \in \Sigma^*$ of length $|w| < \mu$ such that w is a nontrivial element of finite order for T.*

PROOF. Obviously it suffices to prove that (i) implies (ii). So let $w \in \Sigma^*$ be a shortest word that is a nontrivial element of finite order for T. If $|w| < \mu$, then we

are done. Hence, assume that $|w| \geqslant \mu$. Since w has finite order modulo T, there exist integers $n \geqslant 0$ and $k \geqslant 1$ such that $w^{n+k} \leftrightarrow_T^* w^n$. From the choice of w we see that $w \leftrightarrow_T^* \lambda$. Hence, $n + k \geqslant 2$. Since T is Church–Rosser, the words w^{n+k} and w^n have a common irreducible descendant modulo T. In particular, w^{n+k} is reducible, and so w^2 is reducible, since $|w| \geqslant \mu$. Thus $w = w_1 w_2 = w_3 w_4$ with $(w_2 w_3, a) \in T$ for some words $w_1, w_2, w_3, w_4 \in \Sigma^*$ and some $a \in \Sigma \cup \{\lambda\}$.

Now $|w_2 w_3| \leqslant \mu \leqslant |w| = |w_1 w_2|$ implying that $|w_3| \leqslant |w_1|$. Hence, there is some word $x \in \Sigma^*$ such that $w_1 = w_3 x$, i.e., $w = w_3 x w_2$. This gives $(xa)^{n+k+1} \leftrightarrow_T^*$ $(x w_2 w_3)^{n+k+1} = x w_2 (w_3 x w_2)^{n+k} w_3 = x w_2 w^{n+k} w_3 \leftrightarrow_T^* x w_2 w^n w_3 = x w_2 (w_3 x w_2)^n w_3 =$ $(x w_2 w_3)^{n+1} \leftrightarrow_T^* (xa)^{n+1}$. If $xa \leftrightarrow_T^* \lambda$, then this shows that xa is another nontrivial element of finite order for T with $|xa| < |x w_2 w_3| = |w|$, thus contradicting the choice of w. On the other hand, if $xa \leftrightarrow_T^* \lambda$, then we have $w^2 = (w_3 x w_2)^2 = w_3 (x w_2 w_3) x w_2$ $\to_T w_3 (xa) x w_2 \leftrightarrow_T^* w_3 x w_2 = w$, i.e., w is a nontrivial idempotent for T, thus contradicting the assumptions about T. Hence, $|w| < \mu$. $\square$

THEOREM 4.2. *The following problem is decidable*:
Input. A finite, monadic, Church–Rosser Thue system T over Σ, and a word $w \in \Sigma^*$.
Question. Is w a nontrivial element of finite order for T?

PROOF. Given T and w, we can easily decide whether $w \leftrightarrow_T^* \lambda$ holds or not [4]. If $w \leftrightarrow_T^* \lambda$, then w is not a nontrivial element of finite order for T.

Assume, that $w \leftrightarrow_T^* \lambda$. From w we can construct a finite state acceptor M_w for the language $\{w\}^+$. From M_w and T we get a finite state acceptor M_w^Δ for the language $\Delta_T^*(\{w\}^+)$ [8] and a finite state acceptor M_T for $\mathrm{IRR}(T)$. By combining M_w^Δ and M_T we finally get a finite state acceptor $M(T, w)$ that recognizes the language $\Delta_T^*(\{w\}^+)$ $\cap \mathrm{IRR}(T) = \{u \in \mathrm{IRR}(T) | \text{ there is a } k \geqslant 1 \text{ such that } w^k \to_T^* u\}$. It follows immediately that w has finite order modulo T if and only if this set is finite. But the cardinality of this set can be computed effectively from $M(T, w)$. $\square$

Because of Lemma 4.1, Theorem 3.6 and Theorem 4.2 now yield our main result.

THEOREM 4.3. *The following problem is decidable*:
Instance. A finite, monadic, Church–Rosser Thue system T over Σ.
Question. Does there exist a nontrivial element of finite order for T?

5. Presentations of free groups. Given a finite, monadic, Church–Rosser Thue system T over Σ, we can decide effectively whether or not the monoid $M = \Sigma^* / \leftrightarrow_T^*$ presented by $(\Sigma; T)$ is a group [5]. If M is a group, then it is a context-free group [18], since $[\lambda]_T$ is a deterministic context-free language [4]. But from Theorem II of Muller and Schupp [18] we see that a finitely generated context-free group is free if and only if it is torsion-free. Here a group is called *torsion-free* if it does not contain any nontrivial element of finite order. Thus, Theorem 4.3 implies the following

THEOREM 5.1. *The following problem is decidable*:
Instance. A finite, monadic, Church–Rosser Thue system T over Σ.
Question. Is the monoid $\Sigma^* / \leftrightarrow_T^*$ a free group?

Observe that it is undecidable, in general, whether a group given by a finite presentation of the form $(\Sigma; T)$ is free or not, since the property of being free is a

Markov property of finitely presented groups [14]. For a finite, monadic, Church–Rosser Thue system T over Σ, the test of whether or not the monoid presented by $(\Sigma; T)$ is a group can be performed in polynomial time [5]. Further, given $w \in \Sigma^*$ we can derive a nondeterministic finite state acceptor for $\Delta_T^*(\{w\}^+)$ by using polynomial space [8]. If the monoid presented by $(\Sigma; T)$ is a group, then w is a nontrivial element of finite order for T if and only if $w \leftrightarrow_T^* \lambda$ and $\lambda \in \Delta_T^*(\{w\}^+)$. Hence, we can check in polynomial space whether or not this group is torsion-free by using Lemma 4.1. Thus, the problem stated in Theorem 5.1 is actually decidable in polynomial space. However, if we restrict our attention to two-monadic Thue systems, then this problem can be solved more efficiently. Here a Thue system T over Σ is called *two-monadic*, if it is monadic, and if the left-hand side of each rule of T is of length two.

LEMMA 5.2. *Let T be a finite, two-monadic, Church–Rosser Thue system over Σ such that the monoid $\Sigma^*/\leftrightarrow_T^*$ is a group. Then the following are equivalent*:
(i) *There exists a nontrivial element of finite order for T.*
(ii) *There is a letter $a \in \Sigma$ such that a has finite order modulo T.*
(iii) *There is a letter $a \in \Sigma$ such that $a^2 \in \mathrm{domain}(T)$.*

PROOF. Since the monoid $\Sigma^*/\leftrightarrow_T^*$ is a group, there are no nontrivial idempotents for T. Hence, if there exists a nontrivial element of finite order for T, then by Lemma 4.1 there is a letter $a \in \Sigma$ such that a has finite order modulo T. On the other hand, if $a \in \Sigma$ has finite order modulo T, then for some $k \geq 2$, the word a^k is reducible modulo T. Since T is two-monadic, this means that $a^2 \in \mathrm{domain}(T)$. Finally, if $a^2 \in \mathrm{domain}(T)$ for some $a \in \Sigma$, then a has finite order modulo T by Lemma 4 of Avenhaus, Book and Squier [1]. T being two-monadic now implies that a is a nontrivial element of finite order for T.   □

This lemma immediately implies the following.

THEOREM 5.3. *The following problem is decidable in linear time*:
Instance. A finite, two-monadic, Church–Rosser Thue system T over Σ such that the monoid $\Sigma^*/\leftrightarrow_T^*$ is a group.
Question. Does there exist a nontrivial element of finite order for T?

A group G that can be presented by a finite, two-monadic, Church–Rosser Thue system is a free product of a finitely generated free group and finitely many finite groups [2]. Hence, the group G is free if and only if it is torsion-free. This gives our final result.

COROLLARY 5.4. *The following problem is decidable in polynomial time*:
Instance. A finite, two-monadic, Church–Rosser Thue system T over Σ.
Question. Is the monoid $\Sigma^*/\leftrightarrow_T^*$ a free group?

REFERENCES

1. J. Avenhaus, R. V. Book and C. Squier, *On expressing commutativity by finite Church–Rosser presentations: a note on commutative monoids*, RAIRO **18** (1984), 47–52.
2. J. Avenhaus, K. Madlener and F. Otto, *Groups presented by finite two-monadic Church–Rosser Thue systems*, Technical Report 110/84, Department of Computer Science, University of Kaiserslautern, 1984.

3. J. Berstel, *Congruences plus que parfaites et langages algébriques*, Séminaire d'Informatique Théorique, Institut de Programmation 1976–1977, pp. 123–147.

4. R. V. Book, *Confluent and other types of Thue systems*, J. Assoc. Comput. Mach. **29** (1982), 171–182.

5. _____, *When is a monoid a group? The Church–Rosser case is tractable*, Theoret. Comput. Sci. **18** (1982), 325–331.

6. _____, *Decidable sentences of Church-Rosser congruences*, Theoret. Comput. Sci. **24** (1983), 301–312.

7. R. V. Book, M. Jantzen and C. Wrathall, *Monadic Thue systems*, Theoret. Comput. Sci. **19** (1982), 231–251.

8. R. V. Book and F. Otto, *Cancellation rules and extended word problems*, Inform. Process. Lett. **20** (1985), 5–11.

9. Y. Cochet and M. Nivat, *Une generalization des ensembles de Dyck*, Israel J. Math. **9** (1971), 389–395.

10. M. A. Harrison, *Introduction to formal language theory*, Addison-Wesley, 1978.

11. J. E. Hopcroft and J. D. Ullman, *Introduction to automata theory, languages, and computation*, Addison-Wesley, 1979.

12. G. Lallement, *On monoids presented by a single relation*, J. Algebra **32** (1974), 370–388.

13. _____, *Semigroups and combinatorial applications*, Wiley-Interscience, 1979.

14. R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Springer, 1977.

15. W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory*, 2nd revised ed., Dover, New York, 1976.

16. A. Markov, *Impossibility of algorithms for recognizing some properties of associative systems*, Dokl. Akad. Nauk SSSR **77** (1951), 953–956.

17. A. Mostowski, Review of [**16**], J. Symbolic Logic **17** (1952), 151–152.

18. D. E. Muller and P. E. Schupp, *Groups, the theory of ends, and context-free languages*, J. Comput. System Sci. **26** (1983), 295–310.

19. M. Nivat (with M. Benois), *Congruences parfaites et quasi-parfaites*, Séminaire Dubreil, 25ᵉ Année, 1971–1972, Algèbre, Fasc. 1, Exp. No. 7, 9 pp., Secrétariat Mathématique, Paris, 1973.

20. F. Otto, *Conjugacy in monoids with a special Church–Rosser presentation is decidable*, Semigroup Forum **29** (1984), 223–240.

FACHBEREICH INFORMATIK, UNIVERSITÄT KAISERSLAUTERN, POSTFACH 3049, 6750 KAISERSLAUTERN, FEDERAL REPUBLIC OF GERMANY