Theoretical Computer Science 16 (1981) 61–73
North-Holland Publishing Company

ON A SPECIAL MONOID WITH A SINGLE DEFINING RELATION*

Matthias JANTZEN

Fachbereich Informatik, Universität Hamburg, D-2000 Hamburg, 13, Fed. Rep. Germany

Communicated by M. Nivat
Received March 1980
Revised June 1980

Abstract. We show that no finite union of congruence classes $[w]$, w being an arbitrary element of the free monoid $\{a, b\}^*$ with unit 1, is a context-free language if the congruence is defined by the single pair $(abbaab, 1)$. This congruence is neither confluent nor even preperfect. The monoid formed by its congruence classes is a group which has infinitely many isomorphic proper subgroups.

1. Introduction

Semigroups and monoids are closely related to the theory of formal languages, especially to regular and context-free languages. The book by Lallement [5] is a good introduction to these kinds of connections.

Like groups, monoids can be nicely defined by presentations $\langle A; \{w_i = v_i \mid i \in I\}\rangle$, where A is a finite (or infinite) set of generators, and I is a (not necessarily finite) index set for the defining relations $w_i = v_i$, each w_i, v_i being an element of the free monoid A^*. The monoid M defined by such a presentation is the quotient monoid of A^* by the finest congruence containing all the pairs (w_i, v_i), $i \in I$.

For example, $\langle a, b; ab = 1\rangle$ is a presentation of the bicyclic monoid.

Another way of looking at finitely presented monoids, in the case A and I are finite sets, is to consider such a presentation as a definition of a finite Thue system. This is done in [2, 3], where different classes of finite Thue systems, such as confluent, preperfect, Church–Rosser, and similar systems, are studied. Sufficient conditions are developed there which assure that a Thue system defines deterministic context-free languages as finite unions of congruence classes. This also shows how the word problem for some of these classes of finitely presented monoids can be decided in linear time.

For a more detailed study of congruences and their relation to context-free languages, the reader is referred to [2, 3] and the literature cited there, as well as to [5].

* This research was supported in part by the National Science Foundation under Grant MCS77-11360 and by the German Academic Exchange Service under Grant NATO 430/402/547/0.

0304-3975/81/0000–0000/$02.50 © North-Holland

According to [1] we will call a monoid which has a finite presentaton with defining relations $w_i = 1$, $i \in I$, a special monoid, where 1 is the unit element, i e., the empty word of the free monoid. In [2] the finite Thue systems determined by presentations of special monoids are called unitary, in [3] they are called trivial. For example, the set $[1] \subseteq \{a, b\}^*$ of words congruent to 1 with respect to the congruence defined by $(ab, 1)$, i.e., [1] is the unit element of the bicyclic monoid, is exactly the restricted Dyck language over one pair of brackets, which is deterministic context free.

There exist special monoids which have an undecidable word problem [1], or whose congruence classes do not define context-free languages [2, 3]. Special monoids with only one defining relation have a decidable word problem [1], but it is still not known whether an arbitrary monoid given by a single defining relation has a decidable word problem. The word problem in groups with one defining relation, however, is decidable [6].

Here we show first that no finite union of congruence classes of the special monoid M defined by $\langle a, b; abbcab = 1\rangle$ is a context-free language.

In order to obtain this result we use simple calculations as well as a deep result in combinatorial group theory, the so-called 'Freiheitssatz' of Magnus [6]. The basic knowledge about context-free languages which is necessary for our purpose is sufficiently contained in the book of Lallement [5].

We then show that the monoid M does not have a finite preperfect or finite confluent presentation. According to the notion of [2, 3] we call a monoid presentation confluent or preperfect if the Thue system determined by its defining relations is confluent or preperfect. This counter-intuitive result is established by mapping M homomorphically into a group of matrices.

We also include results about the structure of the monoid M, which is in fact a group, showing that this monoid has infinitely many isomorphic proper submonoids.

2. Notation

We use the notation of [5] and [6] and herewith recall the basic definitions we will need.

Given an alphabet X, let X^* denote the free monoid on X. X^* is the set of all words, including the empty word 1, under the monoid operation of concatenation.

If two words $u, v \in X^*$ coincide symbol by symbol, we write $u \equiv v$. Thus $\equiv$ denotes equality in the free monoid X^* and is distinguished from the usual equality = in groups or other monoids. A monoid M is said to have the presentation $\langle X; \{w_i = v_i \mid i \in I\}\rangle$, if M is the quotient monoid of X^* by the finest congruence containing all the pairs (w_i, v_i), $w_i, v_i \in X^*$, $i \in I$.

If the sets I and X are finite, then M is said to be finitely presented. The relations $w_i = v_i$, $i \in I$, are called defining relations and the elements of X are called generators. According to [1] we shall call a monoid M special if all its defining relations are of the form $w_i = 1$, $i \in I$.

If two words $u, v \in X^*$ are in the same class modulo the congruence given by the defining relations of a monoid presentation for M, we shall write $u = v$ and say that u is congruent to v in M. Thus the relation $=$ coincides with the Thue congruence $\leftrightarrow^*$ used in [2, 3]. For any word $w \in X^*$, $[w] := \{u \mid u = w\} \subseteq X^*$ denotes the congruence class of w and is a language in the sense of formal language theory. The definition of regular (or rational, respectively) context-free (or algebraic) languages can be found in [5].

As done for Thue systems in [2, 3], we define the notion of confluent and preperfect monoid presentations.

Let $P = \langle X; \{w_i = v_i \mid i \in I\}\rangle$ be a monoid presentation. For all words $w, v \in X^*$ we write $w \rightarrow v$ (respectively, $w \mapsto v$) iff there exists a defining relation $w_i = v_i$ in P such that $w = \alpha w_i \beta$, $v = \alpha v_i \beta$, $\alpha, \beta \in X^*$ and $\lg(w) > \lg(v)$ (respectively, $\lg(w) \geq \lg(v)$), where $\lg(w)$ denotes the length of the word w. By $\rightarrow^*$ (respectively, $\mapsto^*$) we mean the reflexive, transitive closure of the relation $\rightarrow$ (respectively, $\mapsto$).

Note that the Thue congruence $=$ is the symmetric, reflexive, and transitive closure of the relation $\mapsto$.

Now we call the presentation P above confluent (respectively, preperfect) if for all $w = v$, $w, v \in X^*$, there exists $z \in X^*$ such that $w \rightarrow^* z$ and $v \rightarrow^* z$ (respectively, $w \mapsto^* z$ and $v \mapsto^* z$).

If $X = \{x_1, \ldots, x_n\}$ is an alphabet, then $X^{-1} := \{x_1^{-1}, \ldots, x_n^{-1}\}$ will be a new alphabet.

The monoid M presented by

$$\langle X \cup X^{-1}; \{w_i = v_i \mid i \in I\} \cup \{a_j a_j^{-1} = 1 \mid 1 \leq j \leq n\}$$
$$\cup \{a_j^{-1} a_j = 1 \mid 1 \leq j \leq n\}\rangle$$

is called the group G with generators $x_i \in X$ and defining relations $w_i = v_i$, $i \in I$. The relations $a_j a_j^{-1} = a_j^{-1} a_j = 1$ are called trivial relations and are uniquely determined by the alphabet X. Thus, as usually done, we write the presentation of the group G shortly as $\langle X; \{w_i = v_i \mid i \in I\}\rangle$, making clear by the context that we mean the group and not the monoid, which would be different from the monoid M above.

Note that in the presentation of a group, the defining relations may contain symbols from the alphabet X^{-1}. Any word $w \in (X \cup X^{-1})^*$ which defines the identity element 1 of such a group, i.e., $w = 1$, is called a relator. A word $w \in (X \cup X^{-1})^*$ is cyclically reduced if the symbols x_i^p and x_i^{-p}, $p = \pm 1$, $x_i \in X$, neither occur consecutively nor as both the first and the last letter in w. For example, $x^{-1}yxyx$ is not cyclically reduced, whereas $xyxy^{-1}x$ is cyclically reduced.

3. No element of the special monoid $\langle a, b; abbaab = 1\rangle$ is a context-free language

A series of easy-to-prove lemmas will give us a specific subset of words which are congruent to 1 in the special monoid M presented by $\langle a, b; abbaab = 1\rangle$. Using the

'Freiheitssatz' we then show that words of the form $(ba)^k$ are not congruent to 1 in M unless $k = 0$. Finally, these two results will show that neither [1] nor any finite union of congruence classes of M is a context-free language. Throughout the rest of this paper M will always be the above-defined monoid.

Lemma 3.1. *The following equations are true in M*:

$$abbaab = bbaaba = baabab = aababb = ababba = babbaa = 1,$$

$$bbaa = abab,$$

$$abba = baab.$$

Proof. Applying the relation $abbaab = 1$ to the word $\overline{abba\underline{ab}}\underline{baab}$ either at the left-hand side or at the right-hand side (indicated by $\overline{\quad\quad}$; respectively, $\underline{\quad\quad}$) yields the equation $abba = baab$. Applying this equation to $abbaab$ we get $abbaab = baabab = ababba = 1$. Now using these equations we find $bbaa = abab$ by inspecting

$$\underline{abab}\overline{\underline{ba}\overline{bbaa\underline{ba}}\underline{abab}}.$$

Lemma 3.1 shows that M is cancellative, and in fact a group, since for a and b there exist words $u, u', v, v' \in \{a, b\}^*$, such that $au = u'a = bv = v'b = 1$.

Lemma 3.6 will show that the six words of length six in Lemma 3.1 are the only words of this length which are equal to 1 in M.

Lemma 3.2. $\forall n \geqslant 0$: $(bbaa)^{2n+1} = b(ba)^{n+1}a$.

Proof. The lemma is trivially true for $n = 0$, so assume the lemma is true for a fixed $m \geqslant 0$. Then

$$(bbaa)^{2(m+1)+1} \equiv bbaabbaa(bbaa)^{2m+1} = bba\underline{abbaab}(ba)^{m+1}a$$
$$= bba(ba)^{m+1}a \equiv b(ba)^{m+2}a,$$

so that the result follows by induction.

Lemma 3.3. $\forall n \geqslant 0$: $bb(bbaa)^n aa = (bbaa)^{4n+1}$.

Proof. From Lemma 3.1 we know $abab = bbaa$, which shows $(ba)^{2n+1} \equiv b(ab)^{2n}a = b(bbaa)^n a$, $n \geqslant 0$. Using Lemma 3.2 we then obtain $bb(bbaa)^n aa = b(ba)^{2n+1}a = (bbaa)^{4n+1}$.

Lemma 3.4. $\forall n \geqslant 0$: $(bb)^n(aa)^n = (bbaa)^{f(n)}$, *where* $f(n) := (4^n - 1)/3$.

Proof. The lemma is certainly true for $n = 0$, so let us assume the lemma to be true for a fixed $m \geqslant 0$.

Then $(bb)^{m+1}(aa)^{m+1} \equiv bb(bb)^m(aa)^m aa = bb(bbaa)^{f(m)}aa = (bbaa)^{4\cdot f(m)+1} \equiv (bbaa)^{f(m+1)}$, where we apply Lemma 3.3.

Now let us define for every $w \in \{a, b\}^*$ the regular language

$$R_w := \{w\}\{bb\}^*\{aa\}^*\{ba\}^*$$

and the language

$$L_w := [w] \cap R_w.$$

Lemma 3.5. $n \geq 0$: $(bb)^n(aa)^n(ba)^{f(n)} \in L_1$.

Proof. Since by Lemma 3.1 $bbaaba = 1$, we have $(bbaa)^{f(n)}(ba)^{f(n)} = 1$, which shows $(bb)^n(aa)^n(ba)^{f(n)} = 1$ by Lemma 3.4. Thus,

$$\{(bb)^n(aa)^n(ba)^{f(n)} \mid n \geq 0\} \subseteq [1] \cap \{bb\}^*\{aa\}^*\{ba\}^* = [1] \cap R_1 = L_1.$$

It will be shown that for all $w \in \{a, b\}^*$,

$$L_w = \{w\} \cdot \{(bb)^n(aa)^n(ba)^{f(n)} \mid n \geq 0\}$$

holds. First we have to show that certain words, namely those of the form $(ba)^k$, cannot be congruent to 1 unless $k = 0$.

Lemma 3.6. $(ba)^k = 1$ *if and only if* $k = 0$.

Proof. If we are able to show that $(ba)^k = 1$ iff $k = 0$ is already true for the group G presented by $\langle a, b; abbaab = 1\rangle$, then the statement of Lemma 3.6 is also true for the monoid M.

In order to successfully apply the 'Freiheitssatz' [6, Theorem 4.10], we change the presentation $\langle a, b; abbaab = 1\rangle$ of the group G into a more suitable presentation by means of Tietze transformations. Tietze transformations do not change the group G defined by the different presentations, and are explained in great detail in [6]. Specifically we introduce the new generator $x = ab$, which step by step gives the following different presentations for the very same group G:

$$\langle a, b; abbaab = 1\rangle; \qquad \langle a, b, x; x = ab, xbax = 1\rangle;$$

$$\langle a, b, x; b = a^{-1}x, xbax = 1\rangle; \qquad \langle a, x; xa^{-1}xax = 1\rangle.$$

Obviously $(ab)^k = 1$ in G iff $x^k = 1$ in the group presented by the single relator $xa^{-1}xax$. This relator is a cyclically reduced word, and we can apply Theorem 4.10 of [6] which for our example reads as follows: If $w \in \{c, d, c^{-1}, d^{-1}\}^*$ is cyclically reduced and contains at least one of the symbols c and c^{-1} as well as one of the symbols d and d^{-1}, in which case we say 'w involves c and d', then every nontrivial relator v in the group presented by $\langle c, d; w = 1\rangle$ also involves c and d. This in our case means that $x^k = 1$ is true iff $k = 0$, since otherwise x^k would be a relator not involving a. Since $(ba)^k = 1$ implies $(ab)^k = 1$, the lemma is completely proved.

As it turns out we are able to prove Lemma 3.6 by an entirely different method, well known in group theory. This method of using a suitable homomorphic image of M by means of matrices will later be used to prove the nonexistence of finite preperfect presentations for M. However, in case of semi-group presentations with one defining relation the result of Magnus [6] seems to be more general and sometimes easier to use, since it can be difficult to find the proper homomorphism.

We now prove the main results of this section.

Theorem 3.7. *For each* $w \in \{a, b\}^*$,

$$L_w = \{w\}\{(bb)^n(aa)^n(ba)^{f(n)} \mid n \geqslant 0\}.$$

Proof. Choose w arbitrary in $\{a, b\}^*$. From Lemma 3.5 we can conclude that $\{w\}\{(bb)^n(aa)^n(ba)^{f(n)} \mid n \geqslant 0\} \subseteq L_w$. Now let $v \in L_w$ be arbitrary, then $v = w$, since $L_w \subseteq [w]$ and $v \equiv w(bb)^{n_1}(aa)^{n_2}(ba)^{n_3}$ for some $n_1, n_2, n_3 \geqslant 0$, since $L_w \subseteq R_w$. Since M is cancellative we derive $1 = (bb)^{n_1}(aa)^{n_2}(ba)^{n_3}$, which forces $n_1 = n_2$ since any word which is congruent to 1 in M must contain the same number of occurrences of a and b. Now $(bb)^{n_1}(aa)^{n_1}(ba)^{n_3} = 1$ and $(bb)^{n_1}(aa)^{n_1}(ba)^{f(n_1)} = 1$ imply $(ba)^{n_3} = (ba)^{f(n_1)}$, and finally give $(ba)^{|n_3 - f(n_1)|} = 1$, which by Lemma 3.6 shows $n_3 = f(n_1)$. Thus indeed, $v \in L_w$ implies $v \in \{w\}\{(bb)^n(aa)^n(ba)^{f(n)} \mid n \geqslant 0\}$, which proves the theorem.

Theorem 3.8. *For any finite set* $S \subseteq \{a, b\}^*$ *the language* $M_S := \bigcup_{w \in S}[w]$ *is not context-free.*

Proof. If M_S were context-free, then the language $L_S := M_S \cap (\bigcup_{w \in S} R_w)$ would be context-free too, since M_S is intersected with a regular set (compare [5, Proposition 2.2). Now $L_S = \bigcup_{w \in S} L_w$, thus $L_S \cap \{w\}\{a, b\}^* = L_w$ would also be context-free for each $w \in S$. But the characterization of L_w in Theorem 3.7 together with the pumping lemma for context-free languages [5, Proposition 1.7] finally shows that L_w, and therefore M_S, cannot be a context-free language.

4. Non-existence of preperfect or confluent presentations

Results from [2, 3] show that there cannot exist finite special presentations for the monoid M which in addition are confluent, since the congruence classes would then be context-free languages, contradicting Theorem 3.8. However, it is easy to see that there does not exist a finite confluent presentation for M at all: we already know that $abba = baab$, but none of these words can be equal to some word v of shorter length, otherwise $vab = 1$ would yield a word equal to 1 but not of length six. Even though this result is also an immediate corollary of Theorem 4.6 below, we state this as

Lemma 4.1 *The monoid M cannot have a finite confluent presentation.*

In order to prove the more general result that the monoid M cannot have a finite preperfect presentation, we need the following technical result about certain valid equations in M.

Lemma 4.2. $\forall n \geqslant 0$: *$a^nb^nba = baa^nb^n$ and $a^nb^nab = aba^nb^n$.*

Proof. We first show $a^nb^nba = baa^nb^n$ by induction on n.

This equation is obviously true for $n = 0$ and $n = 1$. Let us assume that the above equation holds for all $0 \leqslant k \leqslant m$, $m \geqslant 1$ fixed. Then

$$\begin{aligned} a^{m+1}b^{m+1}baa &\equiv a^{m+1}b^{m}\underline{bbaa} = a^{m+1}b^{m}abab \equiv aa\underline{a^{m-1}b^{m-1}ba}bab \\ &= aaba\underline{a^{m-1}b^{m-1}bab} = a\underline{abab}aa^{m-1}b^{m-1}b = \underline{abba}aa^{m}b^{m} \\ &= baa\underline{baa^{m}b^{m}} = baaa^{m}b^{m}ba \equiv baa^{m+1}b^{m+1}a, \end{aligned}$$

where the underlined subwords are the ones to which already proven equalities are applied.

Now, since M is a group, $a^{m+1}b^{m+1}baa = baa^{m+1}b^{m+1}a$ shows by cancelling the symbol a at the right-hand side that the equality in question is also true for $k := m+1$.

The second equality of the lemma, $a^nb^nab = aba^nb^n$, is certainly true for $n = 0$ and $n = 1$ and, for $n \geqslant 1$, can be reduced to the first equality as follows:

$$a^nb^nab \equiv aa^{n-1}b^{n-1}bab = abaa^{n-1}b^{n-1}b \equiv aba^nb^n.$$

As an immediate consequence of Lemma 4.2 we see that the presentation $P := \langle a, b; \{abbaab = 1, abba = baab, bbaa = abab\}\rangle$ for M is not preperfect, since none of the defining relations in P can be applied to either word of the equation $aabbba = baaabb$ without increasing their length.

In order to generalize this observation let us first show how the existence of a finite preperfect presentation for M implies a certain equality of words. We will then show later that no such equality can be valid.

Lemma 4.3. *If the monoid M has a finite preperfect presentation, then there exist $n \geqslant 1$ and a word $w \not\equiv a^nb^n$ such that* $\lg(w) = 2n$ *and* $w = a^nb^n$.

Proof. Assume that $S = \langle a, b; \{w_i = v_i \mid 1 \leqslant i \leqslant k\}\rangle$ is a preperfect presentation for M. Let r be the length of the longest word involved in the defining relations of S. From Lemma 4.2 we know $a^rb^rba = baa^rb^r$, and since S is preperfect there exists a defining relation $w = v$ in S, such that $r \geqslant \lg(w) \geqslant \lg(v)$ and w is a subword of a^rb^rba. Since $w \in \{a\}^*$ as well as $w \in \{b\}^*$ implies $w \equiv v$ there are only two nontrivial possibilities for the form of w.

Case 1. $w \equiv b^ta$. In order that $w = v$ be a nontrivial defining relation, we must have $v \equiv b^kab^s$ for some $s \geqslant 1$, $k + s = t$. But this implies $ab^s = b^sa$ and therefore $a^sb^s \equiv a^{s-1}ab^s = a^{s-1}b^sa = b^sa^s$, as stated.

Case 2. $w \equiv a^n b^m$ for some $n, m \geqslant 1$. This shows $a^{n+m} b^{n+m} \equiv a^m w b^n = a^m v b^n$. If $\lg(w) = \lg(v)$, then this is the statement of the lemma; otherwise, $\lg(w) = \lg(v) + 6 \cdot k$ for some $k \geqslant 1$, so that $a^{n+m} b^{n+m} = a^m v b^n (abbaab)^k$ satisfies the statement.

Let us now define the two matrices

$$A := \begin{pmatrix} -\frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B := \begin{pmatrix} -2 & 3 \\ 0 & 1 \end{pmatrix}.$$

It is easy to verify that the matrix product $ABBAAB$ is equal to the identity matrix, so that the following result is immediate.

Lemma 4.4 *If h is the homomorphism defined by $h(a) := A$, $h(b) := B$, then $w = v$ implies $h(w) = h(v)$.*

Lemma 4.4 now yields the second proof for Lemma 3.6: $(ba)^k = 1$ would imply

$$(BA)^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

which is not true for $k \neq 0$, since

$$BA = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \quad \text{yields } (BA)^k = \begin{pmatrix} 1 & 3 \cdot k \\ 3 & 1 \end{pmatrix}.$$

We now proceed towards the main theorem of this section, and show the following lemma.

Lemma 4.5. *If $a^n b^n = w$ for some $w \not\equiv a^n b^n$, then $\lg(w) > 2n$.*

Proof. The following equalities are proved easily by induction on $n \geqslant 0$.

$$A^n = \begin{pmatrix} (-2)^{-n} & 0 \\ 0 & 1 \end{pmatrix}, \qquad B^n = \begin{pmatrix} (-2)^n & 1-(-2)^n \\ 0 & 1 \end{pmatrix}.$$

Thus, if $h(a) := A$, $h(b) := B$ is the homomorphism from Lemma 4.4 and g is the function defined for any integer z by $g(z) := (-2)^z$, then

$$h(a^n b^m) = A^n B^m = \begin{pmatrix} g(m-n) & g(-n) - g(m-n) \\ 0 & 1 \end{pmatrix}.$$

Now consider an arbitrary word $w \in \{a, b\}^*$, then $w \equiv a^{n_1} b^{m_1} a^{n_2} b^{m_2} \cdots a^{n_k} b^{m_k}$ with $k, n_2, \ldots, n_k, m_1, \ldots, m_{k-1} \geqslant 1$ and $n_1, m_k \geqslant 0$. It is straightforward to calculate

$$h(w) = \begin{pmatrix} F & G \\ 0 & 1 \end{pmatrix},$$

where

$$F := g(M_k - N_k), \qquad G := \sum_{j=0}^{k-1} g(M_j - N_{j+1}) - \sum_{j=1}^{k} g(M_j - N_j),$$

$$M_0 := 0, \qquad M_j := \sum_{i=1}^{j} m_i \quad \text{and} \quad N_j := \sum_{i=1}^{j} n_i$$

for $1 \leq j \leq k$. The entry G in $h(w)$ can be rewritten as

$$G = g(-N_1) + \sum_{j=1}^{k-1} [g(M_j - N_{j+1}) - g(M_j - N_j)] - F.$$

Now, if $a^n b^n = w$, then $N_k = M_k$ follows from counting the number of symbols a (respectively, b) in w, and

$$h(a^n b^n) = \begin{pmatrix} 1 & g(-n)-1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} F & G \\ 0 & 1 \end{pmatrix} = h(w)$$

by Lemma 4.4. Thus $F = 1$ and $(G+1) \cdot g(n) = 1$. If we further assume that $\lg(w) \leq 2n$, then $N_k = M_k \leq n$ so that

$$\begin{aligned} 1 &= (G+1)g(n) \\ &= g(n)g(-N_1) + g(n) \cdot \sum_{j=1}^{k-1} [g(M_j - N_{j+1}) - g(M_j - N_j)] \\ &= g(n - N_1) + \sum_{j=1}^{k-1} [g(n + M_j - N_{j+1}) - g(n + M_j - N_j)]. \end{aligned}$$

Since $n \geq N_j$ for all $1 \leq j \leq k$ and $M_j \geq 1$ for all $1 \leq j \leq k-1$, we find that each term under the summation symbol is an even integer, so that the total sum can be equal to 1 only if $g(n - N_1)$ is odd. But this can happen only if $N_1 := n_1 = n$, in which case $g(0) = 1$, $k = 1$, and therefore only if $w \equiv a^n b^n$. Thus, if we assume $a^n b^n = w$ but $w \not\equiv a^n b^n$, then certainly $\lg(w) > 2n$.

Putting Lemma 4.3 and Lemma 4.5 together gives the main result of this section.

Theorem 4.6. *The monoid M cannot have a finite preperfect presentation.*

5. Some structural properties of the monoid *M*

Let us first mention that the mapping h_x, defined for each integer x by

$$h_x(a) := \begin{pmatrix} -\frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad h_x(b) := \begin{pmatrix} -2 & x \\ 0 & 1 \end{pmatrix},$$

induces a homomorphism from M into a group of matrices, since $h_x(abbaab)$ is always equal to the identity matrix. Moreover, we believe that h_x is indeed an isomorphism unless $x = 0$. So far we do not have a proof for this conjecture. In order to develop more properties of the monoid (or group) M, we must again use equalities in M instead of matrix calculations. For instance, if h_x is indeed an isomorphism, we could immediately show that $wv = vw$ for all words w and v, each of which has the same number of occurrences of the symbols a and b, i.e., w and v are elements of the unrestricted Dyck set, which is the unit element $[1]$ of the monoid presented by $\langle a, b; \{ab = 1, ba = 1\}\rangle$.

Using Lemma 4.2 we are however able to show that a large number of words, other than ab and ba, also commute in M.

Lemma 5.1. $\forall n, k \geq 0$: $a^nb^nb^ka^k = b^ka^ka^nb^n$.

Proof. If $k = 1$, then this equation is true by Lemma 3.1.

If $k = 2r$ is even, $r \geq 1$, then

$$\begin{aligned} a^nb^nb^{2r}a^{2r} &= a^nb^n(abab)^{f(r)} && \text{(by Lemma 3.4)} \\ &= (abab)^{f(r)}a^nb^n && \text{(by Lemma 4.2)} \\ &= b^{2r}a^{2r}a^nb^n , \end{aligned}$$

where $f(r) := \frac{1}{3}(4^r - 1)$ as in Lemma 3.4.

If $k = 2r + 1$ is odd, $r \geq 1$, then

$$\begin{aligned} a^nb^nb^{2r+1}a^{2r+1} &= a^nb^nbb^{2r}a^{2r}a \\ &= a^nb^nb(abab)^{f(r)}a && \text{(by Lemma 3.4)} \\ &= a^nb^n(ba)^{2\cdot f(r)+1} \\ &= (ba)^{2\cdot f(r)+1}a^nb^n && \text{(by Lemma 4.2)} \\ &= b^{2r+1}a^{2r+1}a^nb^n. \end{aligned}$$

Lemma 5.2. $\forall n, k \geq 0$: $a^nb^na^kb^k = a^kb^ka^nb^n$ *and* $b^na^nb^ka^k = b^ka^kb^na^n$.

Proof. We only verify the first equality; the second one can be similarly shown.

The equality $a^nb^na^kb^k = a^kb^ka^nb^n$ is obviously true for $n = k$, $n = 1$ and $k = 1$. Thus we assume $n \neq k$, $n = k + r$, $r \geq 1$ (the case $k = n + r$ is symmetric). Now

$$a^nb^na^kb^k = a^ka^rb^rb^ka^kb^k = a^kb^ka^ka^rb^rb^k = a^kb^ka^nb^n.$$

We summarize the previous results by

Theorem 5.3. $wv = vw$ *for all* $w, v \in \{a^nb^n, b^na^n, (ab)^n, (ba)^n \mid n \geq 1\}$.

As an application of Theorem 5.3 we will show that the monoid M contains infinitely many proper submonoids which are isomorphic to M. Since we know that M is in fact a group, we will freely use inverse elements.

Lemma 5.4. $\forall w \in \{a^nb^n, b^na^n, (ab)^n, (ba)^n \mid n \geqslant 0\}$: $wa^{-1}waw = 1$.

Proof. If $w \equiv (ab)^n$, then $(ab)^n a^{-1}(ab)^n a(ab)^n = (ab)^n(ba)^n(ab)^n = (abab)^n(ba)^n =$ 1, using Lemma 4.2. If $w \equiv (ba)^k$, then

$$(ba)^k a^{-1}(ba)^k a(ba)^k = (ba)^{k-1}b(ba)^k a(ba)^k \equiv b(ab)^{k-1}(ba)^k(ab)^k a$$

$$= b(ab)^{k-1}(ba)^{k-1}(ab)^{k-1}abbaa = babbaa = 1.$$

If the lemma is true for $w \equiv a^nb^n$, then $a^nb^na^{-1}a^nb^naa^nb^n = 1$ implies $1 = b^na^{-1}a^nb^naa^nb^na^n = b^na^na^{-1}b^na^nab^na^n$, so that the lemma would also be true for $w \equiv b^na^n$. Now assume the lemma to be true for $w \equiv a^mb^m$. Then

$$1 = ababba = aba\underline{a^mb^ma^{m-1}b^ma^{m+1}b^m}bba$$

$$\equiv a\underline{baa^mb^m}a^{m-1}b^ma^{m+1}b^mbba = aa^mb^mbaa^{m-1}b^ma^{m+1}b^mbba$$

$$\equiv a^{m+1}b^{m+1}a^mb^m\underline{a^{m+1}b^{m+1}ba} = a^{m+1}b^{m+1}a^mb^mbaa^{m+1}b^{m+1}$$

$$= a^{m+1}b^{m+1}a^{-1}a^{m+1}b^{m+1}aa^{m+1}b^{m+1}.$$

Therefore, by induction, the lemma is true for all $w \equiv a^nb^n$, $n \geqslant 0$.

Theorem 5.5. *The monoid M contains infinitely many proper submonoids isomorphic to M.*

Proof. For each $n \geqslant 1$ we define a homomorphism $h_n : \{a, b\}^* \to \{a, b\}^*$ by $h_n(a) := a$, $h_n(b) := a^nb^{n+1}$. We find

$$h_n(a^{-1}) = h_n(bbaab) \equiv a^nb^{n+1}a^nb^{n+1}aaa^nb^{n+1}$$

$$= a^nb^nbaa^{n-1}b^{n-1}bbaaa^nb^nb$$

$$= a^nb^na^{n-1}b^{n-1}baa^nb^nbbaab = bbaab = a^{-1},$$

so that $h_n(a^{-1})$ and a^{-1} define the same element. Also, for all $x, y \in \{a, b\}^*$, $x \not\equiv y$ implies $h_n(x) \not\equiv h_n(y)$. From Lemma 5.4 we conclude that $x = y$ iff $h_n(x) = h_n(y)$, so that h_n induces a one-to-one homomorphism g_n from M into M by $g_n([w]) := [h_n(w)]$ for each $w \in \{a, b\}^*$.

Note that the set of words $h_n([w])$ does not necessarily coincide with the set $[h_n(w)]$, since $h_n(ba) \equiv a^nb^nba = baa^nb^n \not\equiv h_n(w)$ for any word $w \in \{a, b\}^*$ and $n \geqslant 1$.

Lemma 5.4 shows that the group presented by $\langle v, a; \{va^{-1}vav = 1\}\rangle$, with $v \equiv h_n(ab)$, is isomorphic to M under the mapping g_n and is a subgroup of M.

If $n \neq m$, then $g_n(M)$ and $g_m(M)$ are different subgroups of M, since $g_n([ab]) = [a^{n+1}b^{n+1}]$ and $g_m([ab]) = [a^{m+1}b^{m+1}]$ are different elements of M. For, if we assume $a^{n+1}b^{n+1} = a^{m+1}b^{m+1}$, then there exists $k > 1$ such that $a^kb^k = 1$. But this would mean $b^ka^k = 1$ and so $b^{2k}a^{2k} = (bbaa)^{f(k)} = (ab)^{2 \cdot f(k)} = 1$ which contradicts Lemma 3.6. This shows that the monoid (or group) M contains infinitely many isomorphic submonoids.

To verify that infinitely many submonoids of M are proper, consider the mappings $g_{3k-1}: M \to M$ for all $k \geqslant 1$. We shall see that the element $[b]$ of M is not an element of $g_{3k-1}(M)$ for every $k \geqslant 1$. Suppose there exists a word $w \in \{a, b\}^*$, such that $b = h_{3k-1}(w)$. Now the number x of occurrences of the symbol b in the word $h_{3k-1}(w)$ must be of the form $x = 3l + 1$ for some $l \geqslant 0$. On the other hand, by definition of h_n, we know that $x = 3k \cdot y$, where $y \geqslant 1$ is the number of occurrences of the symbol b in w. This gives us the equation

$$3 \cdot k \cdot y = 3 \cdot l + 1$$

which is not true for any choice of integers k, y, and l.

6. Concluding remarks

Despite some unsolved questions about the special monoid M presented here, we think that the method of applying group theoretical results to certain semigroup presentations (or equivalently, Thue systems) has been shown to be quite powerful and might be useful for other examples as well. For, if S and S' are two presentations of the same semigroup, then S and S', considered now as group presentations, also define the same group. The converse, however, is not true.

We do not know whether methods like this are powerful enough to solve open questions like: Is it decidable whether a finitely presented semigroup has some finite confluent presentation? Is it decidable whether a given semigroup presentation is preperfect? What is the complexity of the word problem in special semigroups with single defining relation $w = 1$?

Also, too little is known about the relationships between context-free languages or grammars and semigroup or group presentations. The recent work in [4] shows a different approach in this direction.

Let us finally add some remarks on the use of terminology which is not consistent in the literature. Thue systems with relations only of the form $(w, 1)$ have been called 'unitary' in [2] and 'trivial' in [3]. Since our results showed that even trivial-looking Thue systems of this form can have a very special and nontrivial structure, we propose to call those Thue systems 'special', according to the early notion for semigroup presentations used in [1] and several other places. Sometimes special Thue systems are also called Dyck systems, and we want to emphasize that this might be misleading if the Thue congruence is not confluent, since it then can be the case that the congruence classes are not context-free languages.

References

[1] S.I. Adjan, Defining relations and algorithmic problems for groups and semigroups, *Proc. Steklov Inst. Math.* **85** (1966); English translation published by American Mathematical Society (1967).

[2] R.V. Book, Confluent and other types of Thue congruences, Research Report, University of California at Santa Barbara (1980); *J.ACM*, to appear.

[3] Y. Cochet, Sur l'algébricité des classes de certaines congruences défines sur le monoide libre, Thèse 3^e cycle, Univ. Rennes (1971).

[4] G. Hotz, Eine neue Invariante für kontextfreie Sprachen, *Theoret. Comput. Sci.* **11** (1980) 107–116.

[5] G. Lallement, *Semigroups and Combinatorial Applications* (Wiley, New York, 1979).

[6] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory* (Wiley, New York, 1966).