Divisibility Problem for one relator Monoids

S.I.Adian
Steklov Mathematical Institute
Gubkina str. 8, 117966 Moscow, RUSSIA
e-mail: `si@adian.mian.su`

We consider monoids presented by one defining relation in 2 generators:

$$M =< a, b;\ aU = bV > . \tag{1}$$

Denote $A_1 = aU$ and $A_2 = bV$.

We say that the word X is *left side divisible* by Y in M if there exists a word Z such that $X = YZ$ in M. The left side *divisibility problem* for M is the requirement to find an algorithm to recognize for any two words X and Y, whether or not X is left side divisible by Y in M?

The following theorem was proved in [1,2,3].

Theorem 1 *The word problem for any 1-relator monoids can be reduced to the left side divisibility problem for monoids M presented in 2 generators by 1 defining relation of the form $aU = bV$. For the solution of this problem it sufficies to find an algorithm to recognize for any word aW (or for any word bW) whether or not it is left side divisible in M by the letter b (accordingly by the letter a).*

Algorithm $\mathfrak{A}$

The algorithm $\mathfrak{A}$ was introduced in [2] for a more general case of monoids presented by any cyclefree system of relations. Here we shall apply this algorithm to the case of the monoid M.

The algorithm $\mathfrak{A}$ was used in several papers for a solution of the left side divisibility problem for monoids M under some additional conditions.

To apply this algorithm one should find another algorithm $\mathfrak{B}$ that decides for any word aW, whether or not the algorithm $\mathfrak{A}$ terminates when applied to aW.

For the given word aW the algorithm $\mathfrak{A}$ finds the uniquely defined *prefix decomposition* which is either of the form

$$aW = P_1 P_2 \dots P_k P_{k+1}, \tag{2}$$

where each P_i is the maximal nonempty proper common prefix of the word $P_i P_{i+1} \dots P_{k+1}$ and the appropriate relator aU or bV, or of the form

$$aW = P_1 P_2 \dots P_k A_{j_k} W_{k+1}, \tag{3}$$

where the prefixes P_i are defined in a similar way, but the segment A_{j_k} is one of the relators of the monoid M. We call the segment A_{j_k} *the head* of the decomposition (3).

Let us describe in details how our algorithm $\mathfrak{A}$ works.

Suppose we have an initial word aW. Consider the Maximal Common Prefix of two words aW and A_1 and denote it by

$$P_1 = MCP(aW, A_1). \tag{4}$$

We have $aW = P_1 W_1$ and $aU = P_1 U_1$ for some W_1 and U_1.

Clearly P_1 is not empty. We consider the following 2 cases.

Case 1. If U_1 is empty, then $aW = aUW_1$. So we have a prefix decomposition of the form (3) for $k = 0$.

In this case the algorithm $\mathfrak{A}$ replaces in aW the segment aU by bV. So we obtain $aW = bVW_1$ in M. Hence aW is left side divisible by b in M.

Case 2. Let U_1 be not empty. Then P_1 is a proper prefix of aU.

If W_1 is empty then aW is a proper segment of the relator aU. It is easy to prove that the proper segment P_1 of aU is not divisible by b in M.

Hence we can assume that U_1 and W_1 both are nonempty. It follows from (4) that in this case they have different initial letters a and b.

In this case to prolong the prefix P_1 of aU in P_1W_1 to the right side we should divide W_1 by b if it starts by a or divide W_1 by a if it starts by b. So the situation is similar to the initial one.

Now in a similar way we consider the nonempty word $P_2 = MCP(W_1, A_j)$, where A_{j_1} is the relator of M which has a common initial letter with W_1.

Suppose $W_1 = P_2W_2$ and $A_j = P_2U_2$. Then again we consider 2 cases.

Case 2.1. If U_2 is empty, then $W_1 = A_jW_1$.

In this case we have the following prefix decomposition of the word aW:

$$aW = P_1A_{j_1}W_2,$$

where A_{j_1} is called *the head*.

Case 2.2. Let U_2 be nonempty.

In this case if W_2 is empty then $aW = P_1P_2$ where P_2 is a proper segment of of the relator A_{j_1}. Hence we obtained for aW a prefix decomposition of the form (2). It is easy to prove that the word P_1P_2 is not divisible by b in M.

Hence we can assume that U_2 and W_2 both are nonempty. It follows from (4) that in this case they have different initial letters a and b.

In this case to prolong the prefix P_2 of A_{j_1} in $P_1P_2W_2$ we should divide W_2 by b if it starts by a, or divide W_2 by a if it starts by b. So the situation again is similar to the initial one.

Hence we can consider the nonempty word $P_3 = MCP(W_2, A_{j_2})$, where A_{j_2} is one of the relators of M which has the common initial letter with the word W_2. And so on. The length of the word W_i is decreasing. So after a finite number of steps either we shall find some prefix decomposition of the form (3) with the head A_{j_k} or we shall stop on some decomposition of the form (2).

It is easy to prove that if the decomposition of aW is of the form (2), then the word aW in M is not left side divisible by b.

If the decomposition is of the form (3), then the algorithm $\mathfrak{A}$ replaces the head A_i in aW by the another relator in (1): aU should be replaced by bV or bV by aU. Hence we get one of the following elementary transformations in the monoid M:

$$aW = P_1P_2 \dots P_k aUW_{k+1} \to P_1P_2 \dots P_k bVW_{k+1} = W'$$

or

$$aW = P_1P_2 \dots P_k bVW_{k+1} \to P_1P_2 \dots P_k aUW_{k+1} = W'.$$

Clearly the result W' of this transformation is equal to aW in M. If the resulting word W' starts by the letter b (this happens only if $k = 0!$), then the algorithm $\mathfrak{A}$ terminates by the positive answer. Otherwise the algorithm $\mathfrak{A}$ repeats the same procedure with the word W'.

Theorem 2 *(see [2]) If the word aW is left side divisible by b in M then the algorithm $\mathfrak{A}(aW)$ terminates with the positive result, and in this case we obtain the shortest proof of the left side divisibility of the word aW by b in M.*

Conjecture 1 *There exists an algorithm $\mathfrak{B}$ that decides for any word aW whether or not the algorithm $\mathfrak{A}(aW)$ terminates.*

Problem 1 *Check if the conjecture 1 is true.*

REFERENCES

1. Adian S.I. (1966). Defining relations and algorithmic problems for groups and semigroups. Proc. Steklov Inst. Math. **85**. (English version published by the American Mathematical Society, 1967).

2. Adian S.I. (1976). Word transformations in a semigroup that is given by a system of defining relations. Algebra i Logika **15**, 611-621; English transl. in Algebra and Logic **15** (1976).

3. Adian S.I. and Oganesian G.U. (1987). On the word and divisibility problems in semigroups with one defining relation. Mat. Zametki **41**, 412-421; English transl. in Math. Notes **41** (1987).

4. Adian S.I. and V.G.Durnev. Decision problems for groups and semigroups. In "Russian Math. Surveys" (Uspechi Mat. Nauk, 2000), vol. 55, No. 2, pp. 207-296.