On Word and Divisibility Problems for Monoids Presented by One Defining Relation

S.I.Adian
Steklov Mathematical Institute
Gubkina str. 8, 119991 Moscow, RUSSIA
e-mail: sia@mi.ras.ru

13 мая 2018 г.

Algorithmic Problems in Mathematics

An algorithmic problem is a problem where a single general method (an algorithm) is required to solve any of a given infinite set of homogenous particular questions depending on some parameters. If the required algorithm does not exist, then we say that this algorithmic problem is *unsolvable* or *undecidable*.

During the long history of Mathematics, mathematicians were using the notion of algorithm in the intuitive sense. Around 1936 several formal definitions of the notion of algorithm were suggested: *Turing machines, recursive functions, Markov algorithms*, etc. All these definitions were proved to be equivalent from the point of view of computability.

A formal definition of the notion of algorithm gives an opportunity to establish the unsolvability of algorithmic problems. Unsolvable decision problems were first discovered in mathematical logic and the theory of algorithms. It was later proved that some earlier formulated well-known algorithmic problems were also undecidable.

Church–Turing thesis:

From the point of view of computability, any algorithm in the intuitive sense is equivalent to some algorithm in the precise sense of any of the computational models mentioned above.

In 1947, A.A. Markov and E. Post proved the existence of a finitely presented monoid (semigroup) with the unsolvable word problem.

This was a negative solution of the problem formulated by A. Thue in 1914 and the first example of an undecidable algorithmic problem formulated in mathematics.

I shall speak on a particular case of the same problem in this talk.

The most natural objects used as initial data and results of the work of algorithms are words in some alphabet.
The *free monoid* (free semigroup) S_m in the generators

$$\Sigma = \{a_1, a_2, \ldots, a_m\}$$

is the set of all words in the alphabet Σ with concatenation as an associative binary operation.

- The empty word 1 represents the unit element of a monoid.
- The length of a word A is denoted by $|A|$.
- Graphical equality of words X and Y is denoted $X = Y$.

A *finitely presented monoid* M in the alphabet Σ is defined by a finite set $\{A_i = B_i\}$ of ordered pairs of words in Σ.

For each pair $A_i = B_i$ we consider two elementary transformations (rewrite rules):

Right $uA_iv \to uB_iv,$

Left $uB_iv \to uA_iv,$

where u and v are arbitrary words.

Two words X, Y in the alphabet Σ are called *equivalent in M* (denoted $X = Y$ in M) if either X and Y are graphically equal or there is a finite chain of elementary transformations of the form

$$X = X_0 \to X_1 \to X_2 \to \ldots \to X_k = Y.$$

Obviously, the relation $X = Y$ in M thus defined is symmetric, transitive and compatible with multiplication.

A finitely presented monoid M can be seen as the quotient of the free monoid S_m by the above equivalence relation.

If every element X of a monoid M has an inverse, that is, an element Y such that $XY = YX = 1$ in M, then M is called a *group*.

Finitely presented groups can be considered as monoids in the alphabet $\{a_1, a_2, \ldots, a_n, a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}\}$ containing the following additional defining relations:

$$a_i a_i^{-1} = 1, \; a_i^{-1} a_i = 1 \; (i = 1, 2, \ldots, n).$$

Here a_i^{-1} is the inverse of the generator a_i.

The Word Problem

The word problem for a given Thue system M (a finitely presented monoid or a group) is the requirement to find an algorithm *to recognize, for any two given words in the alphabet of* M, *whether or not they are equivalent in* M.

This problem was formulated first for groups by M. Dehn in 1912 and later by Thue for any Thue system in 1914.

In 1947, almost simultaneously, A. Markov and E. Post constructed finitely presented monoids (Thue systems) with the undecidable word problem.

Based on the results of Markov, P.S. Novikov published in 1955 the first example of a finitely presented group with the undecidable word problem. Simplified proofs of Novikov's result were given later by W.W. Boone, J. Britton, V.V. Borisov and others.

After the results of Markov and Post several authors found simpler examples of finitely presented monoids with the undecidable word problem.

In 1956 G.S. Tseitin constructed an example of a Thue system with the unsolvable word problem presented by 7 short defining relations:

$$ac = ca,\ ad = da,\ bc = cb,\ bd = db,$$
$$eca = ce,\ edb = de,\ cca = ccae.$$

It is the simplest known presentation of a Thue system with the unsolvable word problem. Tseitin used the result of Novikov by reducing the word problem for any finitely presented group to the word problem for this particular Thue system.

Later on, Yu. V. Matiyasevich proved the existence of a Thue system with the unsolvable word problem presented by only 3 defining relations, but one of the relations of his system is very long.

In 1969 V.V.Borisov proved the existence of a group with unsolvable word problem presented by 12 defining relations. This is the minimal known number of relations for groups with unsolvable word problem.

The positive solution of the word problem for all one-relator groups was given by W. Magnus in 1932. For two-relator groups the problem is still open.

On the other hand, Yu.G. Kleiman in 1982 showed that there is a variety of groups presented by only one identity whose relatively free group has the undecidable word problem.

Yu.G. Kleiman. *On the identities in groups.* Proceedings of Moscow Mathematical Society, vol. 44, 1982, p. 62–108.

Word and divisibility problems for one relator monoids

If an algorithmic problem is hard to solve for the general case (or is unsolvable) one usually considers some interesting special cases of the problem. Very often special cases of an algorithmic problem that differ only by small values of a parameter may have different solutions. Some of them may be decidable and others undecidable.

The word problem for one-relator monoids is a very interesting open question. It has been studied by the author for a long time. A positive solution of the word problem was given for two substantial classes of relations:

1. $U = 1$ (for arbitrary U),
2. $U = V$ (for nonempty U and V where the equation is noncancellable on both sides).

The relation $U = V$ for nonempty U and V is called *left side (right side) noncancellable if U and V have distinct initial (final) letters*.

The general case of the word problem for 1-relator monoids can be reduced to the case when the relation $U = V$ is *left noncancellable* (that is, U and V have distinct initial letters).

S.Adian, G.Oganesian, On the word and divisibility problems in semigroups with one defining relation. Mat. Zametki **41**, 412-421, 1987.

For this case the word problem can be reduced to the so-called *left divisibility problem*. We say that a word W is left divisible by D if $W = DX$ for some word X.

Let M be a monoid presented by a left noncancellable relation. In 1976 we published a simple algorithm (*denoted by* $\mathfrak{A}$) which, for an arbitrary given word W and a letter b, finds the shortest proof of the equation $W = bX$ provided that such a word X exists. But we have no method to find in the general case whether the algorithm terminates.

We conjectured that the left divisibility problem, and hence the word problem, is solvable for any monoid M presented by a left noncancellable relation, and that algorithm $\mathfrak{A}$ might be useful for a solution of the problem.

Now we consider monoids presented by one defining relation in two generators:

$$M = \langle a, b \mid aU = bV \rangle. \tag{1}$$

The *word problem for M* is the requirement to find an algorithm to recognize for any two words X and Y whether $X = Y$ in M.

A word X is *left divisible* by a word Y in M if there exists a word Z such that $X = YZ$ in M.

The *left divisibility problem* for M is the requirement to find an algorithm to recognize for any two words X and Y whether X is left divisible by Y in M.

Theorem

- *The word problem for any one-relator monoid can be reduced to the left divisibility problem for monoids* M *presented in two generators by one defining relation of the form* $aU = bV$.
- *For the solution of this problem it is sufficient to find an algorithm to recognize for any word* aW *(or for any word* bW*) whether it is left divisible in* M *by* b *(respectively, by* a*) or not.*

Algorithm $\mathfrak{A}$

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

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

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 $P_i P_{i+1} \dots P_{k+1}$ and the appropriate relator aU or bV,
or of the form

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

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).

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

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

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 two 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 divisible by b in M.

Case 2. If U_1 is not empty, then the first letters of the words W_1 and U_1 should be different.

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

Hence we can assume that both U_1 and W_1 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 $P_1 W_1$ 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 $P_2 = MCP(W_1, A_1)$, where A_1 is the relator of M which has a common initial letter with W_1.

Suppose $W_1 = P_2 W_2$ and $A_1 = P_2 U_2$. Then again we consider two cases.

Case 2.1. If U_2 is empty, then $W_1 = A_1 W_2$.

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

$$aW = P_1 A_1 W_2,$$

where A_1 is *the head*.

Case 2.2. Let U_2 be nonempty.

In this case if W_2 is empty then $aW = P_1 P_2$ where P_2 is a proper segment of of the relator A_1. Hence we obtained for aW a prefix decomposition of the form (2). It is in this case also possible to prove that the word $P_1 P_2$ 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.

To prolong the prefix P_2 of A_1 in $P_1P_2W_2$ in this case 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 $P_3 = MCP(W_2, A_2)$, where A_2 is one of the relators of M which has a common initial letter with the word W_2. And so on.

The length of the words W_i is decreasing. So after finite number of steps either we shall find some prefix decomposition of the form (3) with the head A_k or we shall stop on some decomposition of the form (2). It is possible to prove that if the decomposition of aW is of the form (2), then the word aW is not left divisible by b in M.

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

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

or

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

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

The following Theorem is proved in [2].

Theorem

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

Problem

Check if Conjecture 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"(Uspekhi Mat. Nauk), 2000, vol. 55, No. 2, pp. 207-296.