MATHEMATICS

A. A. FRIDMAN

1962

SovietRxiv

Abstract

Full Text

MATHEMATICS

A. A. FRIDMAN

DEGREES OF UNSOLVABILITY OF THE IDENTITY PROBLEM IN FINITELY PRESENTED GROUPS

(Presented by Academician P. S. Novikov on 14 VI 1962)

In the present work we shall consider the reducibility (with respect to solvability) of algorithmic problems (a.p.) by means of unrestricted Post tables (^{1}). If an a.p. A_1 is reducible (in the sense indicated above) to an a.p. A_2, and the a.p. A_2 is reducible to the a.p. A_1, then one says that these problems have one and the same degree of unsolvability. It is known that there exist different degrees of unsolvability of algorithmic problems (^{1}).

P. S. Novikov constructed the first example of a finitely presented group with an unsolvable word identity problem (^{2}). We use another proof of the existence of a finitely presented group with an unsolvable word identity problem, given by Boone in (^{3}).

At the Fourth Mathematical Congress A. I. Mal' tsev posed the question: what degrees of unsolvability can the identity problem have in finitely presented groups. My attention to this problem was drawn by S. I. Adian. He conjectured that, using Boone's construction (^{3}), one can construct a finitely presented group having any prescribed degree of unsolvability of the identity problem. This conjecture has been confirmed. The main result of the work is Theorem 1, which answers the question posed by A. I. Mal' tsev.

Theorem 1. *For every degree of unsolvability α one can specify a finitely presented group $\mathfrak{B}_\alpha$ in which the word identity problem has degree of unsolvability α.*

An analogous result for associative systems was previously obtained by G. S. Tseitin *.

The proof of Theorem 1 and of the other assertions of this note is omitted on account of their length.

The first part of the work contains a result concerning Turing machines. Let $\mathfrak{M}_1$ be a Turing machine with alphabet of external memory (tape): $s_0, s_1, \dots, s_n$ (where s_0 is the blank symbol) and alphabet of internal states $e_0, e_1, \dots, e_m$ (e_1 is the initial state, e_0 the final state).

Consider on the tape the minimal neighborhood E of the scanned cell outside which the tape is blank. Suppose that in the cells of this neighborhood there are written, from left to right, the symbols

$$s_{i_1} s_{i_2} \dots s_{i_r} \qquad (r \geqslant 1) \tag{1}$$

(r is the number of cells of the neighborhood E, including the scanned one), that the machine $\mathfrak{M}_1$ is in the internal state e_α ($0 \leqslant \alpha \leqslant m$), and that the ρ-th cell of the neighborhood E is being scanned.

To this complete state ** of the machine $\mathfrak{M}_1$ we associate the word

$$h s_{i_1} s_{i_2} \dots s_{i_{\rho-1}} e_\alpha s_{i_\rho} \dots s_{i_r} h \tag{2}$$

(where h is a symbol not belonging to the alphabet of the machine), called the Post word corresponding to the given complete state. The complete state of the machine at any given moment is uniquely determined by the corresponding Post word, and from the Post word the complete state of the machine $\mathfrak{M}_1$ is uniquely recovered.

Theorem 2. *Let α be the degree of unsolvability of an enumerable set M of natural numbers. One can construct a Turing machine $\mathfrak{M}_2$ for which the algorithmic problem: given an arbitrary complete state Q, to recognize whether $\mathfrak{M}_2$ will pass from Q to the internal final state q_0 or not, has degree of unsolvability α.*

According to (4) there exists a Turing machine $\mathfrak{M}_{1-1}$ computing the function $f(m) = 1$, whose domain of definition is M. Let the external-memory alphabet of the machine $\mathfrak{M}_{1-1}$ be s_0, s_1, and the alphabet of internal states be $e_0, e_1, \dots, e_n$. The machine $\mathfrak{M}_2$ is constructed from $\mathfrak{M}_{1-1}$ as follows. The external-memory alphabet of the machine $\mathfrak{M}_2$ consists of the alphabet of the machine $\mathfrak{M}_{1-1}$: $s_0, s_1; e_0, e_1, \dots, e_n$, and the auxiliary symbols $\bar{s}_0, \bar{s}_1, \bar{e}_0, \bar{e}_1, \dots, \bar{e}_n, h, H$. In the alphabet of internal states of $\mathfrak{M}_2$: $q_0, q_1, q_2, \dots, q_k$, three types of states are distinguished: printing, checking, and final.

Definition. A **deductive chain of Post words** (d.c.P.w.) is a word

$$h\bar{Q}_0 h\bar{Q}_1 h \dots h\bar{Q}_{mh}, \tag{3}$$

satisfying two conditions:

---

* This result was reported on 3 XII 1961 at the seminar on constructive mathematical logic at Moscow State University.

** The complete state of the machine $\mathfrak{M}_1$ at each given moment is determined by specifying: the neighborhood E, the word (1), the internal state, and the scanned cell.

1. $h\bar{Q}_0h$ is the initial Post word of the machine $\mathfrak{M}_{1-1}$, i.e. the Post word corresponding to the recording of a natural number in the standard position (4).
2. $h\bar{Q}_ih$ (where $i = 1, 2, \dots, m$) is a Post word immediately following the Post word $h\bar{Q}_{i-1}h$ (i.e. the complete state Q_i of the machine $\mathfrak{M}_{1-1}$ is obtained from the complete state Q_{i-1} in one step of the operation of the machine $\mathfrak{M}_{1-1}$).

The number m will be called the **rank** of the d.c.P.w. (3).

Suppose that on the tape there is printed a d.c.P.w. of rank p, framed by two letters H; $\mathfrak{M}_2$ is in a printing state and scans the right-hand letter H. Then we shall say that the machine $\mathfrak{M}_2$ is in a canonical state of rank p.

The commands of the machine $\mathfrak{M}_2$ are constructed so that, if $\mathfrak{M}_2$ is in a canonical state, then $\mathfrak{M}_2$ erases the H located in the scanned cell, extends the d.c.P.w. of rank p to a d.c.P.w. of rank $p+1$, writes the letter H on the right, and passes into one of the checking states—into the state of searching for the nearest letter H on the left. Having found it, $\mathfrak{M}_2$ passes into a checking state: whether the word enclosed between the two letters H is a deductive chain of Post words. Having checked this, $\mathfrak{M}_2$, in the case of a positive answer, passes into a canonical state of rank $p+1$. Then the entire described cycle of operation is repeated. It is clear that, in further operation, $\mathfrak{M}_2$ will successively pass into canonical states of ever higher rank with one and the same first Post word in the d.c.P.w. If the check gives a negative answer, then $\mathfrak{M}_2$ stops.

For every complete state P one can specify such an $l(P)$ that, if $\mathfrak{M}_2$ began operation from the complete state P and after $l(P)$ steps of operation has not stopped and has not passed into a canonical state, then $\mathfrak{M}_2$ will not pass from the complete state P into the internal state q_0. If $\mathfrak{M}_2$ began operation from a canonical state K, then $\mathfrak{M}_2$ will arrive at the final state q_0 if and only if the function $f(n)$ is defined for the argument n_0 represented in the first Post word of the d.c.P.w. of the canonical state K.

Let $\mathfrak{M}_3$ be an arbitrary Turing machine with external-memory alphabet $s_0, s_1, \dots, s_{m_1}$, internal-state alphabet $q_0, q_1, \dots, q_k$, and with some commands (we do not write them out). Using the construction

Boone' s (^{3}): from $\mathfrak{M}_3$ one can construct the following associative system $\mathfrak{A}$. The alphabet of the system $\mathfrak{A}$ is obtained from the alphabet $\mathfrak{M}_3$: $s_0, s_1, \dots, s_{m_1}; q_0, q_1, \dots, q_k$, by adding the letters s_{m_1+1}, q_{k+1}, q.

The defining relations of the system $\mathfrak{A}$ are divided into two classes (A) and (B):

$$
\text{(A)}\left\{\begin{aligned}
q_0 s_j &= q_0, \\
q_0 s_{m_1+1} &= q_{k+1}, \\
s_j q_{k+1} &= q_{k+1}, \\
s_{m_1+1} q_{k+1} &= q,
\end{aligned}\right.
$$

where $j = 0, 1, \dots, m_1$.

The class (B) contains the relations:

$$
\left.\begin{aligned}
s_m q_i s_j &= q_{i'} s_m s_j, \\
s_{m_1+1} q_i s_j &= s_{m_1+1} q_{i'} s_0 s_{j'}
\end{aligned}\right\}
\quad \begin{gathered}\text{if among the commands of the machine } \mathfrak{M}_3 \text{ there is} \\ \text{the command } q_i s_j \Rightarrow q_{i'} s_{j'} L, \quad j' \neq 0,\end{gathered}
$$

where $m = 0, 1, \dots, m_1$;

$$
\left.\begin{aligned}
s_m q_i s_j s_t &= q_{i'} s_m s_0 s_t, \\
s_{m_1+1} q_i s_j s_t &= s_{m_1+1} q_{i'} s_0 s_0 s_t, \\
s_m q_i s_j s_{m_1+1} &= q_{i'} s_m s_{m_1+1}, \\
s_{m_1+1} q_i s_j s_{m_1+1} &= s_{m_1+1} q_{i'} s_0 s_{m_1+1}
\end{aligned}\right\}
\quad \begin{gathered}\text{if among the commands of the machine } \mathfrak{M}_3 \text{ there is} \\ \text{the command} \\ q_i s_j \Rightarrow q_{i'} s_{j'} L, \quad j' = 0,\end{gathered}
$$

where $t, m = 0, 1, \dots, m_1$;

$q_i s_j = q_{i'} s_{j'}$, if among the commands of the machine $\mathfrak{M}_3$ there is the command $q_i s_j \Rightarrow q_{i'} s_{j'} C$,

$$
\left.\begin{aligned}
q_i s_j s_m &= s_j q_{i'} s_m, \\
q_i s_j s_{m_1+1} &= s_j q_{i'} s_0 s_{m_1+1}
\end{aligned}\right\}
\quad \begin{gathered}\text{if among the commands of the machine } \mathfrak{M}_3 \text{ there is} \\ \text{the command } q_i s_j \Rightarrow q_{i'} s_{j'} R, \quad j' \neq 0,\end{gathered}
$$

where $m = 0, 1, \dots, m_1$;

$$
\left.\begin{aligned}
s_t q_i s_j s_m &= s_t s_0 q_{i'} s_m, \\
s_{m_1+1} q_i s_j s_m &= s_{m_1+1} q_{i'} s_m, \\
s_{m_1+1} q_i s_j s_{m_1+1} &= s_{m_1+1} q_{i'} s_0 s_{m_1+1}, \\
s_m q_i s_j s_{m_1+1} &= s_m s_0 q_{i'} s_0 s_{m_1+1}
\end{aligned}\right\}
\quad \begin{gathered}\text{if among the commands of the machine } \mathfrak{M}_3 \text{ there is} \\ \text{the command} \\ q_i s_j \Rightarrow q_{i'} s_{j'} R, \quad j' = 0,\end{gathered}
$$

where $t, m = 0, 1, \dots, m_1$

(i.e., to each command of the machine $\mathfrak{M}_3$ there corresponds in $\mathfrak{A}$ a group of defining relations).

Lemma 1. *Suppose the recognition problem: whether* $\mathfrak{M}_3$*, from an arbitrary complete state* Q*, will pass into the internal final state* q_0*, has degree of unsolvability* α*. Then the identity problem for the fixed word* q *in* $\mathfrak{A}$ *has degree of unsolvability* α*.*

Definition. A word Z of the system $\mathfrak{A}$ is called **normal** if

$$Z \supset Z_1 q_\xi Z_2 \quad (\xi \supset \Lambda, 0, 1, \dots, k+1),$$

where Z_1, Z_2 are words not containing the letters q_ξ $(\xi \supset \Lambda, 0, 1, \dots, k+1)$.

Number the defining relations of the system $\mathfrak{A}$ and write them briefly as

$$\Sigma_i = \Gamma_i, \qquad i = 1, 2, \dots, \lambda. \tag{4}$$

It is easy to see that Σ_i, Γ_i are normal words. Construct, from $\mathfrak{A}$ according to (1), the Boone group $\mathfrak{B}$.

The positive alphabet of the group is

$$\left\{ \begin{array}{l} s_0, s_1, \dots, s_{m_1+1};\ q_0, q_1, \dots, q \\ t, k, x, y;\ r_1, r_2, \dots, r_\lambda;\ l_1, l_2, \dots, l_\lambda \end{array} \right\}$$

Defining relations*

$$\begin{array}{cccc} & \Sigma_i = l_i \Gamma_i r_i, & (I) & \\ s_j l_i = y l_i y s_j, & (II) & r_i s_j = s_j x r_i x, & (IIa) \\ s_j y = y^2 s_j, & (III) & x s_j = s_j x^2, & (IIIa) \\ l_i t = t l_i, & (IV) & r_i k = k r_i, & (IVa) \\ y t = t y, & (V) & x k = k x, & (Va) \\ & q^{-1} t q k = k q^{-1} t q, & (VI) & \end{array}$$

where $i = 1, 2, \dots, \lambda;\ j = 0, 1, \dots, m_1 + 1$.

In (^{4}) the following theorem is proved.

Theorem 3. Let Σ be an arbitrary normal word. In order that $\Sigma = q$ in $\mathfrak{A}$, it is necessary and sufficient that

$$t \Sigma k \Sigma^{-1} t^{-1} \Sigma k^{-1} \Sigma^{-1} = 1 \quad \text{in } \mathfrak{B}.$$

Using Theorem 3, one can show that Lemma 2 holds.

Lemma 2. The identity problem for the fixed word q in $\mathfrak{A}$ is reducible to the identity problem in the group $\mathfrak{B}$.

Denote by G the group obtained from $\mathfrak{B}$ by deleting relation (VI).

Theorem 4. In the group G the identity problem for words is decidable.

* **Definition.** Let $Z = Z_1 k^\sigma Z_2 k^{-\sigma} Z_3$ be a word of the group $\mathfrak{B}$ (where $\sigma = \pm 1$, and Z_2 contains no letters k^σ). We shall say that in the word Z the distinguished letters k^σ and $k^{-\sigma}$ **cancel each other in the group** $\mathfrak{B}$, if there exists a word Z_4, containing no letters k^σ, and such that

$$Z_1 k^\sigma Z_2 k^{-\sigma} Z_3 = Z_1 Z_4 Z_3 \quad \text{in } \mathfrak{B}.$$

Lemma 3. In order that $Z = 1$ in $\mathfrak{B}$, it is necessary that all letters k^σ of the word Z cancel each other in the group $\mathfrak{B}$.

Let us call **problem A** the problem of finding an algorithm which determines, for each pair of adjacent mutually inverse letters k^σ and $k^{-\sigma}$ ($\sigma = \pm 1$) of any word Z, whether they cancel each other in $\mathfrak{B}$ or not.

Lemma 4. The identity problem for words in $\mathfrak{B}$ and problem A have one and the same degree of unsolvability.

Theorem 5. Problem A is reducible, by means of unrestricted Post tables, to the identity problem for the fixed word q in the system $\mathfrak{A}$.

From Lemmas 1, 4 and Theorems 4, 5, Theorem 1 follows.

In conclusion I express my gratitude to S. I. Adian for his advice and attention to the work.

Received
2 VI 1962

References

1. E. L. Post, Bull. Am. Math. Soc., **50**, 284 (1944).
2. P. S. Novikov, Tr. Matem. inst. im. V. A. Steklova AN SSSR, **44** (1955).
3. W. W. Boone, Ann. Math., **70**, No. 2 (1959).
4. S. K. Kleene, *Introduction to Metamathematics*, Moscow, 1957.

* We omit the trivial relations of the group $\mathfrak{B}$.

Note: Figure translations are in progress. See original paper for figures.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.