ON THE COMPLEXITY OF SOME PROBLEMS FOR GROUPS AND SEMIGROUPS

MATHEMATICS

1970

SovietRxiv

Abstract

Full Text

UDC 51.01:518.5:519.45

MATHEMATICS

Z. K. LITVINTSEVA

ON THE COMPLEXITY OF SOME PROBLEMS FOR GROUPS AND SEMIGROUPS

(Presented by Academician P. S. Novikov, 4 IX 1969)

In this note we establish "complexity" analogues of results obtained earlier by L. A. Bokut' ([2]), Collins ([1]), and Shepherdson ([6]) for the degrees of undecidability of certain algorithmic problems in group theory and semigroup theory. To obtain these analogues (as also in ([4,5])), one carefully analyzes and estimates those reduction processes from which the main results of the indicated works follow; moreover, the original constructions have to be modified in such a way as to ensure the maximum simplicity of the reductions.

Definitions of all "complexity" notions (such as a space signalizing function; reduction with space at most $\varphi_1(n)$ and queries at most $\varphi_2(n)$; computation (and reduction) without stretching, etc.) may be found in ([4,5]).

We shall use the following notation: $|W|$ is the length of the word W; $S_{\mathfrak{M}}(n)$ is the space signalizing function of the Turing machine $\mathfrak{M}$; $\asymp$, $\ll$ denote, respectively, equality and inequality in order (i.e. up to a constant); $W =_\Gamma W'$, $W \simeq_\Gamma W'$ are equality and conjugacy of the words W, W' in the group Γ; "$(?W, W')\, W =_\Gamma W'$" is the word problem in the group Γ; "$(?W, W')\, W \simeq_\Gamma W'$" is the conjugacy problem in Γ; "$(?W)\, W =_\Gamma \widetilde{W}$" is the individual word problem in Γ for the word $\widetilde{W}$ (i.e. the problem: for an arbitrary word W, determine whether it is equal in Γ to the fixed word $\widetilde{W}$); "$(?W)\, W \simeq_\Gamma \widetilde{W}$" is the individual conjugacy problem in Γ for the word $\widetilde{W}$.

We shall say that a problem A has an optimal (space) signalizing function $\sigma(n)$ if: 1) for every Turing machine $\mathfrak{M}$ solving the problem A, $S^{\mathfrak{M}}(n) \gtrsim \sigma(n)$; 2) there exists a machine $\mathfrak{M}_0$ solving the problem A for which $S^{\mathfrak{M}_0}(n) \lesssim \sigma(n)$.

1. The starting point of our work was the theorem ([1,2]), whose statement we give in terms convenient for us.

Theorem A. *For every recursively enumerable (r.e.) predicate $\Gamma(n)$ there exists a finitely presented (f.p.) group $G(\Gamma)$ for which: 1) the word problem is decidable; 2) the problem "$(?W, W')\, W \simeq_{G(\Gamma)} W'$" is reducible to $\Gamma(n)$; 3) $\Gamma(n)$ is reducible to the problem "$(?W, W')\, W \simeq_{G(\Gamma)} W'$" .*

The refinement of this result obtained by us is as follows:

Theorem 1. *For every r.e. predicate $\Gamma(n)$ there exists an f.p. group $G(\Gamma)$ for which: 1) the word problem is decidable without stretching; 2) the problem "$(?W, W')\, W \simeq_{G(\Gamma)} W'$" is reducible to $\Gamma(n)$ without stretching, with queries*

$$\lesssim \frac{|W| + |W'|}{2};$$

3) $\Gamma(n)$ is reducible to "$(?W, W')\, W \simeq_{G(\Gamma)} W'$" with space

$$\lesssim 2n.$$

It follows from this theorem that the "complexity" hierarchy of recursive sets is sufficiently fully modeled in the conjugacy problem for f.p. groups. In particular, the following is true.

Assertion. For any monotone space signaling function $S(n)$ there exists a group G for which the conjugacy problem has an optimal signaling function $\sigma(n)$ such that

$$\sigma(2k) = \sigma(2k+1) \asymp S(2k).$$

Hence it is clear that for even values of the argument the complexity of the conjugacy problem in G coincides exactly with $S(n)$, while for odd values there is a certain "shift" ; it remains an open question whether this shift can be eliminated. Nevertheless, if $S(n)$ grows no faster than an exponential function, then $\sigma(n)$ coincides (in order) with $S(n)$.

2. Collins in ([1]) gives a generalization of Theorem A:

Theorem B. For any r.e. sequence of r.e. degrees $\{d_i\}$ and an r.e. degree d such that $d \geq d_i$ for all i, there exists a f.p. group $G(\{d_i\}, d)$ for which: 1) the word problem is decidable; 2) the conjugacy problem has degree d; 3) for each i there exists a word W_i such that the problem "$(?W)\, W \approx_G W_i$" has degree d_i; 4) the set of degrees of the individual conjugacy problems consists of all finite unions

$$d_{i_1} \cup \ldots \cup d_{i_m}, \quad d_{i_k} \in \{d_i\}$$

(including also degree 0 as the empty union).

This theorem, in particular, shows that any r.e. sequence of degrees of unsolvability can be realized in individual conjugacy problems for one and the same group. We have established (see below Theorems 2 and 3) that an analogous situation also arises for an r.e. sequence $\{S_i(n)\}$ of space signaling functions. Consider, for example, the sequence $n, n^2, n^3, \ldots, n^i, \ldots$.

Then there exists a group in which every individual conjugacy problem has an optimal computation, and the set of optimal space signaling functions of these problems coincides exactly with the set of functions $\{n^i\}$, $i = 1, 2, \ldots$. This example is a special case of the following theorem:

Theorem 2. For any monotone space signaling functions $S(i, n)$ and $\sigma(n)$ ($\sigma(n) \geq \max_{+\leq} S(i, x)$), there exists a f.p. group G possessing the following properties: 1) the word problem for G is decidable without stretching; 2) the conjugacy problem in G has an optimal signaling function $\sigma_G(n)$, and $\sigma_G(2k) = \sigma_G(2k+1) \asymp \sigma(2k)$; 3) for any i there exists a word W_i for which the individual conjugacy problem has an optimal signaling function $\sigma_{W_i}(n)$ such that

$$\sigma_{W_i}(2k) = \sigma_{W_i}(2k+1) \asymp S_i(2k) *;$$

4) for any word $\widetilde{W}$, the problem "$(?\widetilde{W})\ W \approx_G \widetilde{W}$" is either decidable without stretching, or there exist some natural numbers $i_1, \ldots, i_k$ ($k > 0$) and constants C_1, C_2, C_3 ($C_1 \geq C_2 \geq 0,\ C_3 \geq 1$) such that a lower estimate of the complexity of solving this problem is the function

$$\max_{j=1,\ldots,k} S_{i_j}\left(\frac{n - C_1}{C_3}\right),$$

and an upper one is

$$\max_{j=1,\ldots,k} S_{i_j}\left(\frac{n - C_2}{C_3}\right).$$

Theorem 2 is a consequence of Theorem 1 and of the following Theorem 3, whose formulation involves the notion of reduction of a certain problem to a finite number of predicates. Without giving exact definitions, let us simply indicate that, just as the notion of a Turing machine with an oracle and the notion of reduction of one problem to another with space $\leq \varphi_1(n)$ and queries $\leq \varphi_2(n)$ were introduced in ([5]), one can introduce the notion of a Turing machine with a finite number of oracles and the notion of reduction of one problem to a finite number of other problems with space $\leq \varphi(n)$ and queries

$$\leq \varphi_1(n), \ldots, \varphi_k(n).$$

$*$ $S_i(n)_{\mathrm{df}} = \lambda n\, S(i, n).$

Theorem 3. For any recursively enumerable sequence of recursively enumerable predicates $\{A_i(n)\}$ there exists a finitely presented group G such that: 1) the identity problem in G is solvable without stretching; 2) for each i there exists

a word W_i for which: a) "$(?W)\, W \underset{G}{\simeq} W_i$" reduces to $A_i(n)$ without stretching with queries $\leqslant |W|/2$; b) $A_i(n)$ reduces to "$(?W)\, W \underset{G}{\simeq} W_i$" with capacity $\leqslant 2n$; 3) for every word $\widetilde{W}$, either the problem "$(?W)\, W \underset{G}{\simeq} \widetilde{W}$" is solvable without stretching, or there exist a tuple $i_1, \ldots, i_k$ $(k > 0)$ and constants C_1, C_2, C_3 $(C_1 \geqslant 0,\ C_2 \geqslant 0,\ C_3 \geqslant 1)$ such that: a) "$(?W)\, W \underset{G}{\simeq} \widetilde{W}$" reduces to $A_{i_1}(n), \ldots, A_{i_k}(n)$ without stretching with queries $\leqslant (|W| - C_1)/2C_3$; b) each of the predicates $A_{i_1}(n), \ldots, A_{i_k}(n)$ reduces to "$(?W)\, W \underset{G}{\simeq} \widetilde{W}$" with capacity $\leqslant 2C_3 n + C_2$.

It remains an open question whether there exists a group G (under the conditions of Theorem 3) for which the problem "$(?W)\, W \simeq W_i$" and the predicate $A_i(n)$ would reduce to one another without stretching, i.e., whether the "shift" in reducibility that occurs in Theorem 3 can be eliminated. Let us note that in other (but analogous) situations one can avoid this difficulty and show that mutual reductions without stretching are possible. Thus, for example, using a certain modification of Shepherdson' s construction, it is comparatively easy to prove the following analogue of Theorem 10 from ([6]):

Theorem 4. For any recursively enumerable sequence of recursively enumerable predicates $\{A_i(n)\}$ there exists a semigroup T such that: 1) for each i there exists a word W_i for which the problem "$(?W)\, W \underset{T}{=} W_i$" and the predicate $A_i(n)$ reduce to one another without stretching; 2) for any $\widetilde{W}$, either the problem "$(?W)\, W \underset{T}{=} \widetilde{W}$" is solvable without stretching, or there exist a tuple $i_1, \ldots, i_k$ $(k > 0)$ and constants C_1, C_2 such that: a) "$(?W)\, \widetilde{W} \underset{T}{=} \widetilde{W}$" reduces to the predicates $A_{i_1}(n), \ldots, A_{i_k}(n)$ without stretching with queries $\leqslant |W| - C_1$; b) for each $j = 1, \ldots, k$, $A_{i_j}(n)$ reduces to "$(?W)\, W \underset{T}{=} \widetilde{W}$" with capacity $\leqslant n + C_2$.

3. Let us outline the proof of Theorem 1 (Theorem 3 is proved in an analogous way).

We used the construction described by Collins in the proof of Theorem A (while the proof of Theorem A itself was not used). This construction, from an arbitrary semigroup T of a special kind, produces a finitely presented group $G(T)$ with solvable identity problem, and the conjugacy problem for $G(T)$ is Turing-equivalent to the identity problem for T. On the other hand, it is not difficult to show that for any recursively enumerable predicate $\Gamma(n)$ there exists a semigroup $T(\Gamma)$ of the above-mentioned special kind such that $\Gamma(n)$ and the identity problem for $T(\Gamma)$ reduce to one another without stretching. Thus, the whole difficulty in proving Theorem 1 consists in estimating the mutual reducibilities of the identity problem in T and the conjugacy problem in $G(T)$.

The principal working tools in the proof were the notions of stable letters ([7]), a standard basis, a stable word, and removable letters ([2,3]). The following remark, made by Bokut ([2]), proved very useful.

Let a group Γ be given with basis $\tilde{\Gamma}$ and a system of regular stable letters $\Sigma = \{p_1, \dots, p_k\}$, and suppose that Γ has a standard basis (see ([3])), i.e., a set $\mathcal{E}$ of words such that every word $W \in \Gamma$ is equal (in the group-

in Γ) to one and only one canonical word $C(W) \in \mathcal{E}$. Let $C(W)$ be found effectively from W.

Then, in order to be able to solve the conjugacy problem in Γ, it is enough to be able to solve the following three problems:

A. The conjugacy problem in the base $\tilde{\Gamma}$.

B. For arbitrary $W, W' \in \tilde{\Gamma}$ (W, W' not conjugate in $\tilde{\Gamma}$), determine whether they are conjugate in Γ.

C. For arbitrary canonical p-incompressible ($p \in \Sigma$) words W, W', determine whether there exists a word $V \in \tilde{\Gamma}$ such that

$$V \cdot W \cdot V^{-1} \underset{\Gamma}{=} W'.$$

In the proof of Theorem 1 one considers a sequence of groups G_0, G_1, G_2, G_3 such that G_3 coincides with $G(T)$, and each of the G_i ($i = 1, 2, 3$) is a group with a system of regular stable letters Σ_i, base G_{i-1}, and has a standard basis. Solving successively problems A, B, C for G_1, G_2, we obtain that the conjugacy problem for G_2 is decidable without stretching.

To obtain such a simple estimate for the decision algorithm, one has to use a special coding for canonical words. Problem B for G_3 also turns out to be decidable without stretching. It is then proved that problem C for G_3 reduces to the identity problem in the semigroup T, and the complexity of this reduction is estimated; here it is rather difficult to show that the oracle queries do not exceed $m/2$, where m is the length of the record of the initial words. The inverse reduction, i.e. the reduction of the identity problem for T to the conjugacy problem for $G(T)$, is estimated comparatively easily. The complete proof of Theorem 1 turns out to be rather cumbersome.

In conclusion I thank B. A. Trakhtenbrot for posing the problems and for valuable advice, and also M. K. Valiev and A. A. Bokut' for their attention to this work.

Institute of Mathematics Siberian Branch of the Academy of Sciences of the USSR Novosibirsk

Received 1 IX 1969

REFERENCES

1. D. J. Collings, *Acta math.*, **122**, 1–2 (1969).

2. L. A. Bokut' , *Algebra and Logic*, seminar, **7**, No. 5, 4 (1968); **7**, No. 6, 4 (1968).

3. L. A. Bokut' , ibid., **5**, No. 5, 5 (1966).

4. M. K. Valiev, ibid., **8**, No. 1, 5 (1969).

5. B. A. Trakhtenbrot, ibid., **8**, No. 1, 93 (1969).

6. J. S. Shepherdson, *Zs. math. Logik und Grundlagen d. Math.*, **11**, 149 (1965).

7. P. S. Novikov, *Tr. Matem. inst. im. V. A. Steklova AN SSSR*, **44** (1955).

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